COSELEC
A DEISTER ELECTRONIC COMPANY
COSELEC.COM.SG

To Supply, Install Electronic RFID Key Management System

Technical Specifications for Key Management System

The Key Management System shall be supplied, delivered, installed and shall meet the following requirements:

The successful candidate must provide the following:

General Requirements for RFID Key Management System

1. The Key Management System shall come complete with powder coated steel housing, steel doors, Control terminal, contactless RFID key slots (cylinders), RFID key tags and web enabled management software.

2. The Key cabinet housing shall come in sizes based on the following:

   - 32/64 Key Cabinet with an automatic roller shutter that is ergonomically designed to maximize space constraints-without swinging cabinet door/s (H600L x W500W x D170 mm)

   The housing should include backplane PCB, back-up batteries and 1 pair of service keys.

3. Each Control Terminal shall be capable of handling up to a total number of 2048 RFID key slots (cylinders), providing 24 hours of reliable key control.

4. Each key, bunch of keys or other valuables to be controlled shall be securely fitted to the contactless RFID key tag.

5. **Users shall present his/her identification to the system terminal, the system upon validation shall indicate with LED lighting around the whole circumference of the correct slot of the authorised key/s to be released to the user.**

6. **The system shall authenticate and release only the designated key/s to the authorized user, while all other keys remain securely retained (locked) and must be designed based on No Business No Access logic.**

7. **System must be able to support dual or triple authorized token key tag withdrawal/return feature for better accountability.**

8. The user ID, date and time related to all key movement events must be automatically recorded and securely stored in the terminal memory (controller's memory).

9. On returning of keys, the user shall present either his/ her identification or **the key tag directly** to the terminal, upon recognising the identification, the system should indicate with LED lighting around the whole circumference of the correct slot for the keys to be returned to. In the event that the key is placed into the wrong slot, the system shall alert the user to remove it and indicate the right slot with LED again to enable correct return.

10. The system shall provide an audit trail by offering comprehensive electronic log and reporting features consisting of:

    a) which key,
    b) which key slot
    c) which cabinet
    d) which time slots
    e) which user assigned to take which key at what time
    f) which key has been taken, by whom and when
    g) which key has been returned, by whom and when

11. **The system must have a minimum warranty of 3 years.**

Control Terminal

The Key Management System must meet the following minimum requirements:

1. The terminal shall be of maximum size (H=230 x W=130 x D=50mm).

2. **It shall have a built-in Multi-Technology reader that reads most of the latest card technology such as mifare 13.56MHz, HID125KHz, iClass 13.56MHz, Deister 125KHz, Casi-Rusco, EM4000, Sony Felica etc..**

3. **The built-in reader shall read the RFID keytag as well for returning automatically instead of selecting on the terminal as to which keyslot to return. (Auto Keytag Return)**

4. Name of the users shall be displayed on the terminal upon presenting his/her identification.

5. **It shall have an ability to view the last status of keys and the user's drawn or returned without complex menu navigation.**

6. It shall be built-in with a contactless smartcard reader, a contactless RFID key tag reader, 5 X 3 keypad including function keys and 4 lines by 20 characters illuminated LCD display.

7. Each terminal shall be able to keep track up to 4000 users, 2048 key slots (Cylinder) and 7000 events.

8. **It shall allow easy customisation to fit client's access control card readers or biometrics (fingerprint, iris scan, vein recognition or facial recognition).**

9. It shall be provided with a single communication port even when interface with biometric or other readers.

10. It shall control the operations of the cabinet such as assigning of key tags, assigning of user's identification, timing of closing the cabinets, administrator emergency release of keys, clock settings, languages settings, bus address settings, contrast settings, and beeper on/off settings.

11. Firmware updates for the terminal shall be available over the Internet, local network, email or CD.

12. History data shall be held in a ring-memory. i.e. in case of memory overflow the earliest data deleted. The deletion of data is stored and recorded in the history data. The terminal may unload its memory overflow onto a connected PC or other network device if so connected to prevent loss of data.

13. It shall have manual override in case of emergency.

32/64 Key System Automated Roller Shutter Cabinet

1. **It shall come with an automatic roller shutter that is ergonomically designed to maximise space constraints-without swinging cabinet door/s.**

2. The roller shutter shall be tamper-proof and made of powder coated ASA material housing.

3. It shall have a dimension of 600L x 500W x 170D mm in size, grey in colour and made of steel.

4. Special tool shall be required to detach the panel from the cabinet back panel.

5. Each cabinet shall be able to hold 32 key tags with the possibility of increasing the cabinet modularly by number of 32 keys slots for each cabinet, up to 1024 key slots per terminal.

6. It must be able to provide minimum RS 232 with other options such as RS 485 or USB interface.

7. **No press button or any manually triggered unlocking is required to release the keys.**

8. Tamper switch must be installed in the cabinet to prevent from unauthorised removal.

9. **There shall be LED on the rim of the key slots to display the location of the keys in the cabinet upon drawing and returning of keys.**

10. It shall be able to work either online or stand-alone.

RFID Key Slots (Cylinders)

The Key Slots (Cylinders) must meet the following requirements:

1. The key slots (Cylinders) must be based on RFID reader with contactless technology

2. **Must be resistant to salt water and salt air from the sea.**

3. The key slots (Cylinders) must be able to hold the key tags with fail-secure solenoids.

4. **LED will be located in and around the circumference of the key slot (Cylinders), highly visible upon drawing and returning of keys.**

5. **Design must not utilized drop bolt design and allow the key tag to be returned easily & secured it even during power / system failure.**

6. **Ability to facilitate easy manual override without the need of any additional tools.**

7. **It shall carry a warranty of 5 years against manufacturing defects.**

Key Tags

The Key Tags must meet the following minimum requirement:

1. **It shall carry a warranty of 10 years against manufacturing defects.**

2. It shall be robustly design and made of polycarbonate or equivalent plastic casing without any cleaning or maintenance required.

3. **It shall be durable and able to resist shock and other impact up to 2m.**

4. **It shall be water and corrosion proof with IP68 rating. Must be resistant to salt water and salt air from the sea.**

5. It shall not have any openings or open contact with the key slot.

6. It shall use 125 kHz RFID or equivalent frequency

7. Each key tag ID must be uniquely represented.

8. The key tag shall have space provision to allow printing of numbers onto the key tag itself.

9. Each key tag shall have the option of installing a special seal for the purposes of assuring tag/ key integrity.

10. **Can be provision as a transponder for access control.**

Key Rings

The Key Rings must meet the following requirement:

1. The spring steel shall be of 25 dia mm in size

2. Optionally, heavy duty key ring shall be made available with Diameter 60mm and 90mm stainless steel

3. The key ring shall be attached to the key tag with special clip-on seals and no tool is required.

4. **The key ring must not be damaged during re-seal/re-arranging of keys**

Key Seals

The Key Seals must meet the following minimum security requirement:

1. **It must be a one-time seal.**

2. **The key seals must not be reusable.**

3. **No special tools shall be required to seal the keys to the key tag**

4. Special security tool must be used in order to break the seals.

5. Numbered seals shall be provided upon request

Web-Based Key Management Software

The Key Management Software must meet the following minimum requirement:

1. The software shall be **web-based** to enable real-time information from the Central Server conveying input and output between the user and the remote server

2. User groups: users can be combined in groups (for department release mode only

3. Department release mode: keyTags can only be taken at the presence of 2 or 3 users, which have to be in different groups

4. Alarm tool and a special report in proxSafe Commander showing all active alarms in the system with the possibility to start an external software or to send emails in case of a defined alarm

5. **One time assignment of a keyTag: the assignment is valid for one time use only**

6. keyTag time profiles: time profiles can be created for the combination of a keyTag and a user. A time span defines, when a keyTag is allowed to be taken (e.g. the day and the duration)

7. It shall run on a Thin client with SQL Database for easier exchange of data. The client shall run on a web browser such as Netscape, MS Internet Explorer, Opera, Mozilla, Firefox, Safari

8. It must be the latest version and compatible with Microsoft Windows NT,2000, XP and Vista.

9. The software shall be password protected with access rights divided into Administrator, Super User and User

10. The software shall log all activities including but not limited to the time and date of the event, username, key(s) removed/returned and the like.

11. The software shall be able to define group in term of "user group" and "key tag group" for easier programming and management

12. **The software shall have Single, Dual and Triple user features for selected key tags to high security premises. This feature will ensure that at any one time, at least 2 or 3 people must present their credentials to draw/return a particular key. The selected key cannot be drawn should the user does not adhere to the above procedure.**

13. The software shall be able to handle reservation of keys for better management

14. The web based software shall be able to define the reason as to why the key is being drawn. The user has to key in the pre-defined code onto the terminal keypad to inform the reason for drawing the keys.

15. The time profile shall be defined in terms of user or key tag based to draw the keys.

16. The software must generate an alarm should the key be overdue and not returned on time. The alarm can be define as the "user time limit exceeded", "key tag time limit exceeded", "key tag duration exceeded".

17. The user shall have the capability to define 28 different alarms/ events based on the following eg.

    - overdue of keys
    - misuse terminal keypad
    - door closed
    - door opened
    - low battery
    - main power failure
    - key returned in wrong slot
    - tamper alert
    - door left open

18. The user shall be able to send periodical reports to the pre-define E-Mail addresses to inform the selected events/ alarms

19. In case of emergency the administrator could release the key tag under the "remote key tag release" function.

20. The software should come with an automatic backup feature to back up all the transacted data.

21. Reservation of keyTags: keyTags can be reserved for a defined time span for a user (much more options than in the FLM module)

22. Graphic overview of all reservations: In a daily, weekly and a monthly view all reservations can be seen at a time, the view can also be filtered for particular keyTags

23. KeyTag reservations via proxSafe mobile: Terminal users can make their own reservations with this web login. Optional the reservations can be acknowledged by a system administrator before they will be active

24. Email notifications for reservations: User will be informed by Email if reservation of keys is not possible.

25. License validity is stored for each user, if the expiry date is upcoming, users get an email for notification in advance, if license is expired users can not take any keyTags anymore.

26. Mileage logging: When returning a keyTag, a mileage value can be entered, this value is shown in the reports

27. Fault Code logging: When returning a keyTag, a fault code can be entered, this value is shown in the reports. A description for this code can be entered in the proxSafe Commander, which will be also shown in the reports.

28. Simple reservation: keyTags can be reserved for a defined time span for a user.

29. **Issue code logging: A code defining the reason for taking the keyTag can be entered at takeout, this will be shown in the reports. A description for this code can be entered in the proxSafe Commander, which will be also shown in the reports**

30. OPC shall provide a standarized platform to enable communication between different protocols and bus-systems

31. It is a standard automation technology to connect sensors, controllers from different manufacturers into one network

32. OPC generates a client server architecture. The OPC server connects different OPC compatible systems and the client allows the administration of information

33. Devices requires an OPC compatible driver

34. Several and different OPC sub-standards are existing. Eg. the specification OPC A/E for alarms and events. Deister uses the OPC DA (data access) which is specified to transmit data with realtime values.

35. **Must Have Auto-Keytag Roaming Feature, allowing users to withdraw Key from site A and returning to Site B, resulting in effective way of monitoring.**

36. **proxSafe webservice: all functions shall be possible in the web interface can be accessed and controlled by external software**

Reports

The reports generated by the Key Management Software must meet the following minimum requirements:

1. It must be able to generate all the reports parameters including, but not limited to :

    a) Key in
    b) Key out
    c) Time when key was taken
    d) Time when key was returned
    e) Date when key was taken
    f) Date when key was returned

2. The System must also be able to generate specific parameters reports.

3. **Report function must be able to design a minimum of 10 customised report formats.**

Power Requirements

The Key Management System shall be powered by 13.8 VDC with Adaptor with minimum 4 hrs battery backup with 12V / 7Ah Gel Cell battery.

Other Features

The system must also include the following features or equivalent:

1. The system shall allow administrator to remotely release any keys.

2. The system must be able to be connected using TCP/IP, RS485, Network or Standalone.

3. The system must be able to do self-diagnostic test upon request.

4. The Cylinder module (Key Slot) must be able to be deployed in other area of application ie. Notebook Management System, Lockers Management System, Weapon Management System, Document Management System.

Quality assurance

Original manufacturer shall be a company specializing in the supply and installation of electronic Key Management System and should at least have 2 years or more of experience in distributing and manufacturing of such equipment.

Original manufacturer company or its authorized dealer/ contractor or subsidiary must be based in Singapore.

Delivery, storage and handling

The awarded contractor must deliver equipment to Subordinate Courts in manufacturer's packaging undamaged, complete with installation instructions.

The awarded contractor must proceed to claim payment without delay after project completion.

Acceptance tests

Acceptance Tests must be conducted on the electronic Key Management System to verify and demonstrate the full compliance of the proposed solution. The Acceptance Tests shall comprise:

- Proposed solution Functionality Tests;
- Proposed solution Performance Tests; and
- All other tests necessary to demonstrate that the proposed solution meets the requirement specifications
- Equipment must be left on site for further evaluation for 2 weeks.

Damages to property

Any damage due to negligence of the awarded supplier or his staff for the purpose of this Contract shall be wholly or solely the responsibility of the supplier and he must make good of such damages immediately at his own expense to the satisfaction of the Authority.

Safety arrangement

The awarded contractor shall be responsible to take every safety precaution to eliminate dangers to his technicians/ workers, staff of the Authority and the general public. All safety guidelines specified by the Ministry of Manpower must be adhered.

Systems commission

The installation of KMS must be commissioned after the following core activities:

- User Acceptance Test is completed successfully
- Training for users of the Systems is completed

The contractor must guarantee that the Systems perform in accordance with the specifications in the ITQ for a Warranty Period of three (3) years from the date of commissioning.

Compliance list

All vendors are required to provide compliance information on the column provided.

Terms of reference		Compliance	
		Yes	No
	General Requirements :		
	1.		
	2. Critical Compliance		
	3.		
	4. Critical Compliance		
	5. Critical Compliance		
	6.		
	7. Critical Compliance		
	8.		
	9.		
	10. Critical Compliance		
	11.		
	12. Critical Compliance		
	Control Terminal		
	1.		
	2.		
	3. Critical Compliance		
	4. Critical Compliance		
	5. Critical Compliance		
	6. Critical Compliance		
	7.		
	8.		
	9.		
	10.		
	11. Critical Compliance		
	Key System Cabinet		
	1. Critical Compliance		
	2.		
	3.		
	4.		
	5.		
	6.		
	7.		
	8.		
	9.		
	10. Critical Compliance		
	11.		
	12. Critical Compliance		
	13. Critical Compliance		
	14.		
	Key Slots		
	1. Critical Compliance		
	2. Critical Compliance		

Terms of reference		Compliance	
		Yes	No
	3. Critical Compliance		
	4.		
	Key Tags		
	1. Critical Compliance		
	2.		
	3. Critical Compliance		
	4. Critical Compliance		
	5. Critical Compliance		
	6.		
	7.		
	8. Critical Compliance		
	9.		
	Key Rings		
	1.		
	2.		
	3.		
	4. Critical Compliance		
	Key Seals		
	1. Critical Compliance		
	2. Critical Compliance		
	3. Critical Compliance		
	4. Critical Compliance		
	5. Critical Compliance		
	Web-Based Key Management Software		
	1. Critical Compliance		
	2.		
	3. Critical Compliance		
	4.		
	5.		
	6.		
	7. Critical Compliance		
	8.		
	9.		
	10.		
	11		
	12 Critical Compliance		
	13		
	14. Critical Compliance		
	15. Critical Compliance		
	17. Critical Compliance		
	18. Critical Compliance		
	19. Critical Compliance		
	20. Critical Compliance		
	21. Critical Compliance		
	22. Critical Compliance		
	23. Critical Compliance		

Terms of reference		Compliance	
		Yes	No
	Reports		
	1.		
	2.		
	3. Critical Compliance		
	Power Requirements		
	Other Features		
	1. Critical Compliance		
	2.		
	3.		
	4. Critical Compliance		

Notice Please note that the compliance list is compulsory. Information not provided will be disqualified accordingly. The Contractor shall provide explicit responses of compliance or non-compliance for this tender. In the event of any non-compliance with the technical requirements, the Contractor shall satisfy the Authority with a write up to explain that the items offered are equivalent to the required. Where the Contractor fails to satisfy the Authority in the manner above, the tender is liable to be rejected.