COSELEC
A DEISTER ELECTRONIC COMPANY

COSELEC.COM.SG

To Supply & Install Electronic Key Management System

Technical Specifications for Key Management System

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

Item	Qty	Description
1		32/64/128/256/384 **RFID** Key Slot (cylinder) Steel Housing Cabinet
2		Control Terminal Built-in Smart Card Reader & **Key Tag Reader (Auto Key Tag Return)**
3		RFID Key Tags with unique ID numbers
4		Key Seals
5		Key Rings
6		Web-Based Management Software (can be installed either as stand-alone or in LAN environment)
7		Necessary Accessories
8		Installation, Testing, commissioning & training

General Requirements

1. The Key Management System shall come complete with powder coated steel key cabinet with clear doors, steel doors or without doors, terminal, contactless RFID key slots (cylinders), key tags and web enabled management software.

2. **The Key cabinet housing shall come in 5 sizes based on the following:**

   - **3U (H285 x 621 x D245 mm) with up to 32 RFID Key Slots (Cylinder)**
   - **6U (H465 x W621 x D210 mm) with up to 64 RFID Key Slots (Cylinder)**
   - **12U (H698 x W621 x D210 mm) with up to 128 RFID Key Slots (Cylinder)**
   - **24U (H1396 x W621 x D210 mm) with up to 256 RFID Key Slots (Cylinder)**
   - **36U (H1920 x W609 x D210 mm) with up to 384 RFID Key Slots (Cylinder)**

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

3. The backplane PCB unit shall include a CPU, 8 port multiplexers, 4 I/O ports, door strike port, control terminal port, 2 tamper switch ports, power In/Out port

4. **The RFID key slot panel shall come in modular of 8/16/32 RFID key slots (Cylinder) and RFID contactless key tags. The Panel shall come in 2 sizes such as 3 height unit or 6 height unit or choice of both as per user requirements to minimise cost**

5. **Each terminal shall be capable of handling up to a total number of 1024 RFID key slots (cylinders), providing 24 hours of reliable key control.**

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

7. **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.**

8. The system shall authenticate and release only the designated key/s to the authorized user, while all other keys remain securely retained (locked).

9. 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).

10. **On returning of keys, the user shall present either his/ her identification or the key tag (Auto-Keytag Return Feature) 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.**

11. 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

12. **The system must have a minimum warranty of 3 years. With a revision of extension of warranty of up to 5 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. Name of the users shall be displayed on the terminal upon presenting his/her identification.

3. **It shall have an ability to view all keys and the user's status.**

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

5. **It shall be able to keep track up to 4096 users, 2048 key slots (Cylinder) and 7000 events.**

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

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

8. 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.

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

10. 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.

11. **It shall have manual override in case of emergency.**

System Cabinet

The System Cabinet must meet the following minimum requirement:

1. **The Key Management System shall come complete with powder coated steel key cabinet with clear doors, steel doors or without doors, terminal, contactless RFID key slots (cylinders), contactless RFID key tags and web enabled management software.**

2. The Key cabinet housing shall come in 4 sizes based on the following:

   - **3U (H285 x 621 x D245 mm) with up to 16/32 RFID Key Slots (Cylinder)**
   - **6U (H465 x W621 x D210 mm) with up to 32/64 RFID Key Slots (Cylinder)**
   - **12U (H698 x W621 x D210 mm) with up to 64/128 RFID Key Slots (Cylinder)**
   - **24U (H1396 x W621 x D210 mm) with up to 128/256 RFID Key Slots (Cylinder)**
   - **36U (H1920 x W609 x D210 mm) with up to 384 RFID Key Slots (Cylinder)**

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

4. The backplane PCB unit shall include a CPU, 8 port multiplexers, 4 I/O ports, door strike port, control terminal port, 2 tamper switch ports, power In/Out port

5. **The RFID key slot panel shall come in modular of 16 RFID key slots (cylinder) and RFID contactless key tags. The Panel shall come in 2 sizes such as 3 height unit or 6 height unit or choice of both as per user requirements to minimise cost**

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 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 technology**

2. **The key slots (Cylinders) must be able to hold the key tags with self- locking fail-secure solenoids. Not utilizing drop bolt design.**

3. **Ring LED shall be utilized to illuminate the circumference of the key slot (Cylinders), allowing high visibility upon drawing and returning of keys.**

4. Drawing and returning of keys must be smooth without any manually activated device/action.

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 made of polycarbonate or equivalent plastic casing without any cleaning or maintenance required.

3. **Must not have any hole on the key tag.**

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

5. **It shall be water and corrosion proof with IP67 rating.**

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

7. It shall use 125 kHz RFID or equivalent frequency

8. **Each key tag ID must be uniquely represented with 128bits combination.**

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

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

Key Rings

The Key Rings must meet the following requirement:

1. It must be made of high grade spring steel.

2. There must be an option range of key ring sizes to select, 25 mm, 60mm or 90mm.

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 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. **No Sealing tools required**

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. It shall run on 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

3. **It must be the latest version and compatible with Microsoft Window 7, 8**

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

5. 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.

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

7. **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 a particular key. The selected key cannot be drawn should the user does not adhere to the above procedure.**

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

9. 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”.

10. The user shall have the capability to define the following different alarms/ events

    - 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

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

12. **The administrators are enabled to release the key tag under the “remote key tag release” function from the software.**

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

14. **Must have well design, field proven structured module for: Key reservation, fleet management, casino module etc.**

15. **Must have properly structured Web Interface & OPC Server Interface module provision for future interfacing with 3rd part software.**

16. **Software must be securely design with SSL and other counter breach measures**

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 back-up with 12V / 7Ah Gel Cell battery.

Other Features

The system must also include the following features or equivalent:

1. **The internal system cabling design must be based on star topology and utilizing RJ45 connector, without utilizing ancient ribbon cable design**.

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 provision for future deployment in other areas 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		
	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		

Terms of Reference		Compliance	
		Yes	No
	2. Critical Compliance		
	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		
	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		
	16. Critical Compliance		

	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.