I.1: Commissioning of electronic key management systems

Security of all types of assets of the Centre is of paramount importance. The very first level of security of various organizational assets is ensured by the secure handling of the physical access to entry/exit gates of the various building premises inside the campus. The physical access to all the buildings premises in the Centre is presently managed using the physical lock and key arrangement. The management of the physical keys of the various buildings in RRCAT is looked after by both central industrial security force (CISF) and the RRCAT Security Section.

The manual key management tasks include: (a) commissioning of manual key distribution system, (b) proper mapping of authorization rights of key issue/deposit of specified buildings to identified persons received vide authorization letters, and (c) ensuring that the authorized person makes an entry in a register for records prior to withdrawal or deposit of the keys. This whole process is time consuming and prone to errors and it is practically impossible to check authorization for each individual, every time a key is withdrawn/deposited. To streamline the management of keys of the various vehicles/office/utility building premises inside the Centre, a comprehensive electronics key management system (EKMS) is commissioned at seven security posts and one in administration building.

EKMS consists of a key holding rack, a card reader and network interface for local area network (LAN) connectivity. Each key, which is dispensed using EKMS is attached to a "key fob" using a stainless steel ring. Each "key fob" has a unique identification number. The function of the card reader is: (a) to read the information stored inside the radio frequency identification (RFID) card that is brought in its proximity and (b) to activate release of the key from the key ring only when authorized RFID card is brought in its proximity. This ensures that only authorized persons can draw/deposit the specific keys for which they are authorized by flashing their respective RFID cards to the EKMS reader. Every EKMS machine is equipped with a battery backup to ensure its working even during power failures. Every EKMS machine can log around 10000 key transactions (withdrawal/deposit) along with date & time stamp information. These transaction records can be downloaded on a personal computer (PC)/laptop only by authorized personnel identified by user name / password using the LAN port of the EKMS. This is helpful in post analysis of any incident involving key management. Presently EKMS machines have been installed at eight locations as mentioned in Table I.1.1.

Table I.1.1: List of buildings where EKMS was commissioned along with the no. of key fobs in each EKMS.

Sr. No.	Name of the building	No. of key fobs
1.	Guard House	16
2.	Indus - 1	16
3.	Magnet Development Lab	16
4.	R & D Block - A	16
5.	R & D Block - C1	16
6.	Colony main gate	32
7.	Palace gate	16
8.	Administration building	64

All the EKMS machines are connected to RRCATNet, the campus wide LAN in RRCAT. Various required management tasks related to these EKMS machines are performed using an EKMS server machine, which is also connected to RRCATNet. In case of any exigency (fire/accident, etc.), personnel of Fire & Safety Section are authorized to withdraw any key from any EKMS station using a master RFID card. Apart from Fire & Safety personnel, Deputy Chief Security Officer (DCSO) & Chief Security Officer (CSO) can also withdraw any key using their respective RFID cards.

Figure I.1.1 shows photographs of the commissioned EKMS machines in three different buildings. The entire task including technology exploration, procurement and commissioning was carried out by the team of seven members of Videography and Electronic Key Management Committee of RRCAT.

Figure I.1.1: Photographs of EKMS machines commissioned at some of the buildings in RRCAT.

Reported by:
Viraj Bhanage (viraj@rrcat.gov.in)