A smart card is a device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. Smart cards have the capability to store large amounts of data, carry out own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart Cards are available in a variety of forms such as plastic cards, key fobs, watches, subscriber identification modules used in GSM mobile phones, and USB-based tokens.

ISO/IEC 14443 and ISO/IEC 7816 standards

Smart card technology must conform to international standards (ISO/IEC 7816 and ISO/IEC 14443). ISO/IEC 14443 is the international standard for contactless smart chips and cards that operate (i.e., can be read from or written to) at a distance of less than 10 cms. This standard operates at 13.56 MHz and includes specifications for the physical characteristics, radio frequency power and signal interface, initialization and anti-collision protocols and transmission protocol. ISO/IEC 7816 is the international standard for contact smart cards.

A contactless smart card

A contactless smart card includes an embedded smart card secure microcontroller or equivalent intelligence, internal memory and a small antenna and communicates with a reader through a contactless radio frequency (RF) interface. This is useful in applications/functions that need to protect personal information and/or deliver fast and secure transactions, such as transit fare payment, government and corporate identification/documents such as electronic passports and visas, and financial payments.

1 Sourced from Smart Card Alliance: http://www.smartcardalliance.org/pages/smart-cards-faq
Some of the areas where smart card technology is used include:

- In the US Personal Identity Verification (PIV) cards are used by all Federal agencies for employees and contractors.
- Contactless transit fare payment systems installed in cities such as Washington, DC, Chicago, Boston, Atlanta, San Francisco and Los Angeles.

Contactless smart cards have the ability to securely manage, store and provide access to data on the card, perform on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a contactless smart card reader.

Contactless smart card systems are closely related to contact smart card systems. Like contact smart card systems, information are stored on a chip embedded within the contactless smart card. However, unlike the contact smart card, the power supplied to the card as well as the data exchanged between the card and the reader are achieved without the use of contacts, using magnetic or electromagnetic fields to both power the card as well as to exchange data with the reader. The contactless smart card contains an antenna embedded within the plastic body of the card. When the card is brought into the electromagnetic field of the reader, the chip in the card is powered on. Once the chip is powered on, a wireless communication protocol is initiated and established between the card and the reader for data transfer.

The following four functions describe at a high level the sequence of events that happen when a contactless smart card is brought near a card reader:

- Energy transfer to the card for powering the integrated circuit (chip)
- Clock signal transfer
- Data transfer to the contactless smart card
- Data transfer from the contactless smart card
Hence, once the card is brought within range of an electromagnetic field of the required frequency, the card will be powered up, ready to communicate with the reader. The card must be within 10 centimetres of a reader for it to be effectively powered; however, the effective range for communications for the card to be read will depend on a number of factors like the power of the reader, the antenna of the reader and the antenna of the card.

**Contactless payment**

Contactless payment is an improvement to the way debit or credit payment is handled when making a purchase. Contactless payment transactions require little to no physical connection between the card and the checkout device. Instead of “swiping” or “inserting” a card, the contactless card is tapped on or held within an inch of a machine that reads the card; with the payment information is sent to the merchant wirelessly. Contactless credit and debit cards include a smart card chip. Contactless credit or debit cards are being issued by a number of financial issuers. (American Express, Chase, MBNA, Citibank, HSBC Bank, Key bank, Wells Fargo, Citizens Bank).

**Security and Privacy**

Smart cards offer a number of features that can be used to provide or enhance protection in systems. The following is a brief description of some of these features and how they can be used to protect privacy.

- **Authentication.** Smart cards provide mechanisms for authenticating others who want to gain access to the card. For example it is possible to ensure that a banking application has been authenticated as having the appropriate access rights before accessing financial data or functions on the card.

- **Secure data storage.** Smart cards provide a means of securely storing data on the card. This data can only be accessed through the smart card operating system by those with proper access rights. The user can have better knowledge and control of when and by whom their personal data is being granted access.
Encryption. Smart cards provide a robust set of encryption capabilities including key generation, secure key storage, hashing, and digital signing. These capabilities can be used by a system to protect privacy in a number of ways.

Strong device security. Smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks.

Secure communications. Smart cards provide a means of secure communications between the card and card readers.

Biometrics. Smart cards provide mechanisms to securely store biometric templates and perform biometric matching functions. These features can be used to improve privacy in systems that utilize biometrics. For example, storing fingerprint templates on a smart card can be an effective way of increasing privacy in a single sign-on system that uses fingerprint biometrics as the single sign-on credential.

Personal device. A smart card is, of course, a personal and portable device associated with a particular cardholder. The smart card plastic is often personalized, providing an even stronger binding to the cardholder. These features can be leveraged by systems to improve privacy.

Certifications. Many of today's smart cards have been certified that they comply with industry and government security standards. They obtain these certifications only after completing rigorous testing and evaluation criteria by independent certification facilities. These certifications help systems protect privacy by ensuring that the security and privacy features and functions of the smart card hardware and software operate as specified and intended.

**Use of Biometrics**

A smart card ID can combine several ID technologies, including the embedded chip, visual security markings, magnetic stripe, barcode and/or an optical
stripe. By combining these various technologies into a smart card ID token, the resulting ID can support both future and legacy physical and logical access applications. They can also support other applications that have traditionally required separate ID processes and tokens.

Also, biometrics are used in many new identity management systems to improve the accuracy of identifying individuals.

Smart cards provide a highly effective mechanism to protect the privacy of an individual that has a requirement to use a biometric identity system.

- The biometric information can be stored on the smart card rather than in an online database, allowing the biometric owner the opportunity to manage the physical possession of the card holding the individual's biometric information.

- The biometric data can be secured with state-of-the-art encryption techniques while providing full three-factor authentication capability at the card/reader level.
  - Something you have – the card with all of its security capabilities
  - Something you know – a password or personal identification number (PIN)
  - Something you are – the biometric

In a non-smart-card-based application, the password or PIN and biometric would be stored in an online database outside the control of the individual and the biometric information would be captured and passed to an application for matching.

- The individual’s biometric can be captured by a reader and passed to the smart card for matching, rather than passing the stored biometric information to the reader for matching. The individual’s biometric information would never leave the card, preventing any possibility of compromise.
Security capabilities of contactless smart cards

Contactless smart cards use RF technology, but, by design, operate at a short range and can support the equivalent security capabilities of a contact smart card chip. Contactless smart cards and readers conform to international standard.

The contactless smart chip includes a smart card secure microcontroller and internal memory and has unique attributes RFID tags lack – i.e., the ability to securely manage, store and provide access to data on the card, perform complex functions (for example, encryption and mutual authentication) and interact intelligently via RF with a contactless reader. Applications using contactless smart cards support many security features that ensure the integrity, confidentiality and privacy of information stored or transmitted, including the following:

- Mutual authentication. For applications requiring secure card access, the contactless smart card-based device can verify that the reader is authentic and can prove its own authenticity to the reader before starting a secure transaction.

- Strong information security. For applications requiring complete data protection, information stored on cards or documents using contactless smart card technology can be encrypted and communication between the contactless smart card-based device and the reader can be encrypted to prevent eavesdropping. Hashes and/or digital signatures can be used to ensure data integrity and to authenticate the card and the credentials it contains. Cryptographically strong random number generators can be used to enable dynamic cryptographic keys, preventing replay attacks.

- Strong contactless device security. Like contact smart cards, contactless smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips
are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis.

- Authenticated and authorized information access. The contactless smart card’s ability to process information and react to its environment allows it to uniquely provide authenticated information access and protect the privacy of personal information. The contactless smart card can verify the authority of the information requestor and then allow access only to the information required. Access to stored information can also be further protected by a personal identification number (PIN) or biometric to protect privacy and counter unauthorized access.

- Support for biometric authentication. For human identification systems that require the highest degree of security and privacy, smart cards can be implemented in combination with biometric technology. Biometrics are measurable physical characteristics or personal behavioural traits that can be used to recognize the identity or verify the claimed identity of an individual. Smart cards and biometrics are a natural fit to provide two- or multi-factor authentication. A smart card is the logical secure storage medium for biometric information. During the enrolment process, the biometric template can be stored on the smart card chip for later verification. Only the authorized user with a biometric matching the stored enrolment template receives access and privileges.

- Strong support for information privacy. The use of smart card technology strengthens the ability of a system to protect individual privacy. Unlike other technologies, smart card-based devices can implement a personal firewall for an individual, releasing only the information required and only when it is required. The ability to support authenticated and authorized information access and the strong contactless device and data security make contactless smart cards excellent guardians of personal information and individual privacy.

It is important to note that information privacy and security must be designed into an application at the system level by the organization issuing the
Contactless device, card or document. It is critical that issuing organizations have the appropriate policies in place to support the security and privacy requirements of the application being deployed and then implement the appropriate technology that delivers those features. The ability of contactless smart card technology to support a wide array of security features provides organizations with the flexibility to implement the level of security that is commensurate with the risk expected in the application.

**Proposed smart card for KCC**

Borrower will be issued a bio-metric enabled smart card with preloaded information on KCC, Land holding, identification etc. The KCC smart card can be used in (a) merchant establishments and (b) BCs. In the case of BC the amount will be limited to Rs 5000 per transaction.