**Security Capabilities Properly Supported by The Smart Card Technology**

Smart cards – cards that have embedded integrated circuits to process information – offer various features that deliver privacy in access-control systems. As with security features of a smart card chip, devices that have contactless smart cards make use of RF technology and can also support similar security capabilities by conforming to security standards such as ISO/IEC 7816 and ISO/IEC 14443. They also have the capability to implement various cryptographic protocols such as RSA, ECC, AES and 3DES.

A smart card chip has a secure microcontroller and holds an internal memory with unique security attributes which RFID tags also lack, such as, ability to carry out complex functions like mutual authentication and encryption; and store, manage and provide data access on the card. Smart card technology supports security capabilities such as confidentiality, integrity and reliability of information systems.

Here is a brief overview of some security aspects of smart cards.

**Authentication**

A smart card only provides access upon authentication of the individual’s identity. It validates a user, device or application that wishes to use the card’s data. For instance, it ensures that a banking application is given access rights before it can access card functions or financial data.

**Secure Storage of Data**

Smart cards also allow secure storage of data so that it can only be accessed by any entity with access rights through the smart card operating system. This feature can help enhance a system’s privacy by storing a user’s personal information on the card instead of a central database. Hence, a user gets better control and knowledge of when and by whom their personal data is accessed.

**Encryption**

One of the key security features of smart cards is encryption. With capabilities such as secure key storage, key generation, digital signing and hashing, they can protect a user’s privacy from all aspects. For instance, smart cards can create digital signatures for email messages, hence enabling users to validate the email’s authenticity. It also prevents anyone to tamper with the message and assures the recipient about the message origin. Also, the indication that the email message was originated from a smart card makes it more credible.

**Information Security**

Applications that need complete data privacy can take advantage of contactless smart cards technology for information stored on cards. This is done by encrypting the data and communication between the smart card device and reader to stop eavesdropping. Digital signatures and hashing authenticate the card’s credibility and credentials. Similarly, random number generators that are strong cryptographically can prevent replay attacks by enabling dynamic cryptographic keys.

**Device Security**

It’s very hard to duplicate smart card technology due to its built-in resistance to tampering. Smart card chips have software and hardware capability to detect and respond to a tampering attempt and to counter potential attacks. For instance, a smart card chip has extra layers of metal, sensors for detecting UV light and thermal attacks, and added hardware and software circuitry to prevent differential power analysis.

**Secure Communication**

Just like security protocols in other networks, smart cards can securely send and receive data in a private, secure manner between the card and the receiver.

**Biometrics**

A smart card can also help in securing systems that use biometrics. With a smart card, you can store biometric templates and use them to carry out biometric matching. The templates can be stored in the smart card chip and used later for verification. Especially for systems that require human identification with a highest degree of privacy and security, smart card and biometric technology can be integrated to create an authentication mechanism, such as two-factor or multi-factor authentication.

For example, if you store fingerprints in a smart card system instead of a central database, it increases privacy in a single sign-on system which uses fingerprint authentication for single sign-on.

**Personal Device**

A smart card also serves as a personal portable device that belongs to a unique cardholder. Each card is personalized with the cardholder’s name on it. Though it’s an obvious feature, it can provide leverage to the [cardholder](http://www.cardzgroup.com/ContactSmartCard.html). For example, a patient’s Personal Health Information (PHI) can be stored on their smartcard instead of the database to protect their privacy and maintain accuracy.

**Personal Privacy**

Smart card technology also allows a system to protect personal privacy of individuals. Contrary to other technologies, a smart-card based device can put a private firewall for the cardholder and only release the information necessary for the reader for that particular time frame.

**Conclusion**

With all the security advantages the smart cards have to offer, it should also be kept in mind that these features need to be integrated into an application at system level by the organizations issuing the card or device. Hence, issuing organizations must have proper mechanism and policies in place to cater to the security requirements of the application under deployment and implement the relevant technology to support the features. This ability of smart cards to support a large number of security features has provided flexibility to the organizations in implementing the required level of security which is in line with the potential risk in the application.