Smart cards – cards with integrated circuits to process information – have a number of security features that simple credit cards or magnetic stripe cards don’t provide. While a normal credit card is just a piece of plastic, a smart card has an embedded microprocessor inside which holds and processes information for authentication. The layout of the chip makes it resistant to tampering, with enough processing power to secure the information it holds, encrypt and execute any instruction from a program with predetermined interface. It can save your valuation information such as passwords, account numbers, private keys or personal information. This is the reason why smart cards have an edge over magnetic stripe cards and are highly secure for financial transactions, identity authentication or providing access control.

Smart cards are now being used worldwide in many applications that include:

**Healthcare:** portable medical records, physician ID cards, health ID cards

**Payments Systems:** [transit fare payment cards](http://www.cardzgroup.com/ContactLessSmartCard.html), contact/contactless debit and credit cards

**Telecommunication:** telephone payment card, SIM

**Secure ID Applications**: citizen identity documents, drivers’ licenses, employee identity badges, electronic passports

Let us look at some of the ways why smart cards help build and enhance security.

**Authentication**

A smart card provides a way to authenticate any third party that needs to access the card. It can validate a user, device or application that wishes to use data on the card’s chip. For example, in case of a bank, this feature ensures privacy by authenticating the bank application’s access to the card before it is allowed to access financial or personal data on the card.

**Access Control**

When selecting an access control system, there can be many options to choose from such as magnetic stripe cards, proximity cards, biometric systems or smart cards. Out of all these options, a smart card may prove helpful as it offers the most features.

Firstly, consider if there is no smart card. Under a usual business, an access control arrangement at the building may have separate controllers than those of the tenant’s and integrating them together can be a hassle. Similarly, consider a university or a hospital in which specific departments or buildings have their separate systems and require different cards for access. Again, this can confuse the user when tracking which card is required for access to a particular facility.

Now comes the smart card. It contains a computer chip that is fed with personal information of the cardholder and the access points that individual is authorized to enter. Since smart cards have added capability of being integrated with diverse technologies that include biometric systems, magnetic strip and proprietary proximity, they can be applicable to a variety of technology readers in different locations.

Not only this, but smart cards also provide logical access control apart from physical access and protect an organization’s information network. In logical access control system, a company’s network is locked for access unless an authorized user inserts a smart card in a card reader which is linked to their workstation. This feature ensures more security than a password system because often employees forget to turn off their systems at the end of the day, leaving them open for anyone to access confidential organizational files. With a smart card however, the card removal will unlink the workstation from the company’s network and lock the logical access from that system.

**Encryption**

Smart cards come with a complete package of encryption capabilities which include secure key storage, key generation, digital signing and hashing. These can be used for protecting privacy in a number of ways. For instance, a smart card can validate the authenticity of an email by producing a digital signature for an email message. This not only secures the message from tampering but also ensures the email recipient about the authenticity of the sender.

**Data Storage Security**

A smart card can also be used for securely storing data that can only be accessed by the operating system of the card by a user with access rights. This feature is useful when instead of storing data on a central database, it is stored on a smart card. In such a case, the card holder knows who is accessing their information, and when.

**Secure Communication**

This works similar to security protocols that are used in many networks. Smart cards ensure secure communication between the reader and the card to send and receive private data in a secure manner without intervention from an outside party.

**Biometric Matching**

Biometric templates and matching functions can be securely stored with the help of smart cards. This feature helps improve privacy in systems that implement biometrics. For instance, storing a fingerprint on smart card instead of central repository is a better way to enhance privacy in a single sign-on system using fingerprint credentials.

**Tamper-Resistant**

It is extremely difficult to forge or duplicate smart card technology, hence, they are highly resistant to tampering attempts. A smart card has a variety of software and hardware capabilities that help counter potential threats.

**Confidentiality**

The personalized nature of a smart card provides a stronger sense of confidentiality to the cardholder. For instance, a healthcare provider may store a patient’s history and prescription information on a smart card as opposed to a paper to ensure that the private information of the patient stays with them.

With so many advantages, markets and organizations that have traditionally used machine-readable card technologies like magnetic stripe and barcode are now increasingly moving towards adopting smart cards, particularly for applications that strictly need security and validation.