**What Are Security Implications for Smart Cards**

Smart cards are typically plastic cards that contain an embedded computer chip that stores and transmits data pertaining to a value, information or both. Nowadays, several commercial sectors like banking and finance, healthcare, media and entertainment are using smart cards system in their applications. They are often used for access control to restricted areas, guarantee payments or prove identity.

**Why Smart Cards?**

Smart cards provide several security features in comparison to basic printed cards or magnetic stripe cards resulting in more secure and efficient applications. They may look like credit cards without stripe, but their functionality is much more secure. Smart cards store information unless accessed by a software program with the right interface in a predetermined way, and upon providing the right second-factor PIN. They also often hold digital certificates of a user to prove their identity during authentication. Even better, instead of handing over the user private key, they provide the proof of correct private key in response to an authentication request.

Smart card technology is also resistant to tampering and is very hard to forge or duplicate. Smart card chips have additional software and hardware capabilities to detect a tampering attempt and react accordingly, thus countering any potential attack and enabling [secure interactions with the overall system](http://www.cardzgroup.com/products.html). They can also be used for secure communication between a card and reader which allows confidential data to be sent in a secure manner and ensures that the data is not intercepted during communication.

**Is Smart Card Security Enough?**

Despite the security features of smartcards, they are still not foolproof. Integrating smart cards into the system gives rise to its own issues regarding security, because the card data can be used far and wide in many applications. Since the system users are given access to the smart card data, it is open to threats from malicious insiders or outside hackers. This is also because only a small percentage of successful attacks have to do with authentication. In fact, the total security breaches that result from bypassing authentication (including cracking, password guessing, replay attacks) only add up to less than 1 percent of successful attacks. Rather, most attacks take place because of phishing attacks or because of unpatched software. In such cases, smart cards security features are not of any help. In most of the cases, a hacker will access the user’s system and authenticate himself as the user of the smart card. In other words, once a computer is compromised, it is easy for a bad guy to steal card credentials and use it as their own. They can do this either by copying digital certificate out of local cache, keylogging user’s PIN or by tampering the card’s client software.

Hackers can also steal identifying information like a ZIP code and then attempt to make an online purchase with a dummy smart card. While doing this they can provide stolen information to validate their identity and then claim a defective chip. This technique has resulted in attracting fraudsters more towards online fraud as compared to POS terminals in the past couple of years.

**Better Smart Card Security – The Way Forward**

To improve smart card security, card issuers and authentication companies are turning to technology such as biometric solutions. In 2017, MasterCard tested smart cards with biometric authentication technology. The card had a biometric scanner in a corner where users can place finger during a transaction. If biometric authentication is successful then the user does not need to provide a PIN or signature. This solution does not need any changes to the merchant software or hardware as it is compatible with all types of EMV-enabled terminals that have finished the Mastercard Terminal Integration Process.

Similarly, Visa has started a pilot program for smart card biometric authentication where a red or green light on the card indicates an unsuccessful or successful match respectively.

In the meantime, Ingenico, a global leader in seamless payments, has established an innovative solution for micro-merchants which is based on a technology known as PIN on Mobile (PoM) or PIN on Glass (PoG). This technology will allow customers to insert their smart cards in a compact reader and enter their PIN manually on the merchant’s personal device. The solution is for both contactless bank cards and EMV and verifies that the device’s execution environment is secure before a PIN is entered by the customer.

Despite the threats they may face from cyber criminals, smart cards offer security like no others. They are better authenticators and less time consuming than long passwords; they are two-factor enabled, and have underlying hash that is formed from complex password to prevent cracking. With technologies like biometric and PoG implemented in smart cards, we can expect a more secure and restricted environment around sensitive information.