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

We asked Scott Richardson, CEO of Cardzgroup, some questions about how smartcards can help build security for organizations.

**What are smart cards?**

“While ‘smart card’ is a broad term encompassing a wide array of technologies, in general a smart card is a credential containing a chip which allows it to store/process/transmit data back to a card reader.”  
  
**How can smart cards help organizations analyze user data?**

“In addition to the obvious use where an organization can analyze logs of where/when each card has been used at a terminal such as a POS kiosk or door access reader, RFID technology in the newer generation of smart cards allows much more interesting data to be gathered. For example, many smart cards now contain UHF (Ultra High-Frequency) antennas which allow them to be read from distances of several meters away – this allows organizations to set up triangulated readers in doorways/larger areas that can track user movements without requiring a card to be individually presented to a reader terminal.”  
  
**How do you see the future of smart cards and how will the smart card industry grow or change?**

“The two areas where smart card technology is most quickly evolving are in security and miniaturization. With the worldwide migration to much higher security EMV banking cards, the newest generation of smart cards are capable of full on-chip cryptography which has significantly increased the security of cards across the industry. In addition, smart cards are increasingly being miniaturized into more diverse form factors such as mini-tags and smart wearables. Both of these trends will continue as the smart card is increasingly used as a two-factor credential in conjunction with phone or biometrics.”

**Will smart cards be obsolete in 10 years? Why or why not?**

“The standard CR80 wallet-sized smart cards will definitely not be as prevalent in 10 years as they are today, but this is because they will increasingly be replaced by smaller and more convenient alternatives. The smart card in its broad definition, meaning a standalone passive physical credential, will almost certainly not be obsolete in the next ten or even twenty years.”

With so many advantages that smart cards have, 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.