

Smartcard Introduction:

Smartcards are not a new technology. The first patent was filed in 1970 by Dr. Kunitaka Arimura of Japan, and the first smartcard was issued in France in 1979. Since then, over a billion cards have been issued, upgraded and replaced world wide. While most smartcards have been deployed in Europe and the Pacific Rim, Americans are seeing and hearing more about smartcards every day. American Express Blue Card, IBM security ads, and even your new building access badge all use smartcard technology. Smartcards are often described by their technology capabilities but they all have one thing in common: Integrated Circuit (IC) chips embedded into a credit-card-sized piece of plastic. These IC chips provide a variety of functionalities, memory capacities and operating systems, but what makes these cards so valuable is the security designed into the chip. While one can never claim that any technology is 100% secure, the amount of time, money and effort required to steal data on these chips is so high that thieves look elsewhere for easier targets.

Types of smartcards:

There are three categories of smartcards:

- 1) Secure Memories
- 2) Microcontrollers (also called microprocessors)
- 3) Cryptocontrollers

Secure memories are the least expensive and least complex. They are not too different than a thumb drive, floppy disk or any other storage media, but they offer security protection that none of these other media can. They are often segmented by their available memory capacity. Currently these chips can store as much as 32K bytes, but there are new chips coming to market on a monthly basis with more and more storage capacity.

The next group of smartcards is the microcontrollers. These are small, sophisticated computers on a single chip, the size of 5mm x 5mm. Specifications include the amount of RAM, ROM, Operating System, bit-length and clock speeds -- exactly how a desktop or laptop computer is specified. Because these are small computers in themselves, they can actually process and calculate data on the chip independent of the computer. This gives the user an added layer of security since confidential data can be kept clear of viruses, spyware and hackers.

Finally there are the cryptocontrollers. These are the most advanced and expensive chips on the market. They are primarily used for applications that utilize advanced encryption algorithms like Public Key Infrastructure (PKI). Cryptocontrollers and PKI applications offer the ability to securely verify, authenticate, and authorize the user. In addition, they can help ensure that the data transmitted is also the data received, thus enabling the legal acceptance of digital signatures.

Power LogOn™ by Access Smart™ can use all of these smartcard chips. We believe in matching the technology to the needs and requirements of the customer. We encourage clients not get too engrossed with the technology, but rather describe what you want to accomplish and why. Then let the smartcard experts help define what smartcard technology is best for your needs.

Uses for smartcards:

Smartcards have created a new paradigm shift. They force the question, "What could I do with a personal computer in my wallet?" Today we have only just started to realize all of the functions for smartcards. The more common applications include payment, telecommunications, network access, loyalty, transit, identification and medical. The key to make any of these applications successful is to clearly identify the value to the customer. Access Smart puts this philosophy into action by offering tools that make the computer experience secure and easy to use. Our first product Power LogOn offers secure data access through convenient password management. By never having to remember or type a password again, and not having your passwords stored on a computer for others to find, individuals can protect their valuable data from falling into the wrong hands.