

UPGRADE THE CARD

What is a Smart Card?

A **Smart Card** is a credit card sized card that contains an embedded micro-processor chip that can be used to not only store data, but can function as an on-board computer to securely complete a transaction. The chip-based technology protects the card-holder's identity in a secure, privacy-enhancing manner.

Smart cards are currently being used world-wide in a number of applications that require high levels of security and data assurance, such as banking, healthcare, transportation, and mobile communications. In the United States, smart card chips are used in the Department of Defense's Common Access Card (also known as the 'CAC' card, the secure ID card all military personnel use), the current e-Passport, and Personal Identity Verification Card (PIV) used by all Federal employees through Homeland Security Presidential Directive -12 (HSPD-12).

The federal government chose to use the smart card as a basis for these applications for one important reason: they are invaluable in preventing fraud. They're secure, they're reliable, and they've been the industry gold-standard in identity management protection for *over thirty years*. But the U.S. government isn't alone: every G-20 nation in the world has adopted smart cards in one form or another to protect their citizen's benefits, identity, financial transactions, or healthcare records.

What Are the Benefits of Smart Cards?

The first and foremost benefit is security. Smart card chips are designed to be tamper-proof and forge-proof, and have proven to be far more reliable than other machine-readable cards, such as those using magnetic stripes or bar codes, which can be easily cloned, spoofed, or copied. The biggest benefit of a smart card is not only that the information on the card is secured, but it ensures the security of the entire network every time it's used. It does this through *authentication*.

What is Authentication and How Does it Work?

According to the dictionary, authentication is *the act of confirming the truth of an attribute of a datum or an entity*. Plainly put, it means **verifying you are who you say you are**.

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something you have, something you know, or something you are. Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, or establishing a chain of trust.

To find out more about smart cards and their uses in identity management, cybersecurity, healthcare, financial services, and entertainment, visit www.SecureIDCoalition.org.

Incorporating at least two of these factors, known as multi-factor authentication, has been determined by security research in both the banking industry and government to be necessary for positive authentication. These factors are:

- “Something you have” – a token, wristband, smart card or cell phone
- “Something you know” – password, PIN, username, challenge/response
- “Something you are” – a biometric such as a fingerprint

Two-factor authentication is a combination of at least two of the three categories listed above. An easy two-factor authentication application to remember is using an Automatic Teller Machine (ATM). The user must have physical possession of a card (something you have) and the associated PIN must be entered (something you know). Both factors provide a higher threshold of security. However, using two-factor authentication with an easily abused technology, like the mag stripe used on all U.S. ATM and credit cards, is like locking your doors against burglars but leaving your windows open.

Because smart cards allow for multi-factor authentication *directly on the card's on-board computer*, and are both tamper- and copy-proof, they provide for the highest degree of identity assurance and fraud prevention.

How can Smart Cards Help Reduce Fraud?

Based on smart cards' exceptional track record with the military's CAC card, ePassport, and the PIV card, Congress is currently considering using them to reduce fraud in the Medicare system.

Authenticating Medicare beneficiaries through a secure smart card system will reduce fraud as it ensures beneficiaries are verified to receive the services, pharmaceuticals, or equipment they are prescribed. The same system also verifies providers are authorized to both provide those services and bill Medicare. The identification and authentication process prevents imposters from posing as either beneficiaries or providers, thus thwarting fraudulent transactions.

Countries all over the world have found healthcare success using smart cards, including the United Kingdom, France, Germany, Italy, Spain, Finland, Belgium, and Luxembourg. Closer to home, leading hospitals and medical centers have already embraced smart card health identity documents. For instance, to protect their patient's health care records from fraud and abuse, Mount Sinai Medical Center has issued over 100,000 smart card credentials which directly contributed to a cost savings of over \$1 million in system wide.