
Posted on Mon, Jan. 17, 2005

With high-cost 'smart cards,' military targets tighter security

By Dan Lee
Mercury News

Call them digital dog tags.

About 4 million "smart cards" that run on software from a Silicon Valley company -- have been issued to every member of the U.S. armed forces and civilian workers in the Department of Defense to use as high-tech ID cards.

The cards are part of a costly and ambitious government-wide drive -- mandated by President Bush in the wake of the Sept. 11 terror attacks -- to use the latest technology for a unified identification system that tightens the security of federal facilities and computer systems. The cards can be used to gain entrance to a high-security building or to use government computers to send encrypted e-mail.

The Defense Department says the cards not only boost security but also help efficiently deploy troops and cut down on paperwork. The military, however, is still learning how to make full use of the cards and their many capabilities.

In fact, the military has abandoned many of the uses first envisioned, such as storing each user's medical and financial information on the card. And the program has been more pricey than expected, costing up to \$1 billion for everything from buying the cards to developing the security technology on them, according to one analyst's estimate.

The cards -- about the size of a driver's license -- carry a photograph along with standard information such as name, rank and Social Security number. But what makes each card "smart" is the embedded computer chip inside used to positively identify its holder for tasks such as logging onto a military computer system.

"It's like a passport," said Rob Brandewie, director of the Defense Manpower Data Center, the agency based in Seaside that oversees the smart card program. "It's the only token we give to everybody who has an association to the DoD."

Among the program's corporate suppliers is Fremont-based ActivCard, which provides much of the software to run the program. In fact, ActivCard moved its headquarters from France to the United States in large part because of its deal with the Department of Defense.

The smart cards are issued from 900 locations in 27 countries for active duty and selected reservists in the Army, Navy, Air Force and Marines along with civilian Pentagon employees and some contractors. The first cards were issued in December 2000, with the program completely rolled out by early 2004. About 10,000 cards are issued each day.

An Army Ranger injured in Iraq who lost his card may be issued a new one from a military hospital in Germany. Sailors may use them to get food on some bases, or to check out equipment.

Smart cards offer "two-factor" authentication: A user inserts the card into a specialized card reader, and then has to enter a personal-identification number before gaining access.

The cards also use the encryption technology called public-key infrastructure, or PKI, to access networks and Web sites instead of using user names and passwords. Many think the cards are more likely to prevent unauthorized access to sensitive government information. The card can also place "digital signatures" for tasks such as filing a travel claim online.

"When I leave my office, I pull the card out of my computer, locking the screen and preventing other people from gaining unauthorized access to the network," Navy Chief Information Officer David Wennergren said in an e-mail.

But some aren't using the cards for much more than an old-fashioned ID.

"I think a lot of guys out in the trenches probably aren't using it for anything at the moment," said Frederick Ziegel, security technology analyst with Soleil Securities Group, who added that there were likely few devices to read the cards

in Iraq.

Since the war began in Iraq, however, the cards have been used to send encrypted e-mail from U.S. Central Command in Florida to military planners in Qatar, said Mary Dixon, deputy director of the Defense Manpower Data Center.

The military is testing other uses. Marine recruits will be able to use an "electronic purse" on the card to make various purchases, such as getting a fresh "high-and-tight" haircut.

The cards are also designed to be used to enter buildings and in combination with biometric identifiers -- such as a fingerprint scan -- to gain access to highly secure areas. But those capabilities are not yet being used on a wide basis.

In some locations, military personnel may have to juggle three or four different cards for entering buildings. The goal is to transfer all of those tasks to the smart cards, Dixon said. This year, the Pentagon will begin issuing cards with 64 kilobytes of space, up from the current size of 32 kilobytes.

The Pentagon's use of the cards as primarily as an identification system is a departure from how it first envisioned smart cards. In the late 1990s, cards in test programs were loaded with personal information such as medical files.

But limited space on the cards and the task of keeping so many cards updated proved difficult, Dixon said.

The biggest concern, however, was to make sure any information on the cards could not endanger military members who were captured. An enemy could possibly find out a soldier had an allergy to a certain medicine, and threaten that person with exposure to it, Dixon said.

"Or if it had a home address, they could threaten the family," she added.

Cards with computer chips are considered more secure than ones using only magnetic strip to store information, said Randy Vanderhoof, executive director of the Smart Card Alliance, an industry group in Princeton Junction, N.J. If stolen, the card would be of little use because the thief would not have the programmed card reader or the personal-identification number needed to access the information.

He added that the chip in the card is designed to self-destruct if tampered with. "It's never been cracked to anybody's knowledge," Vanderhoof said.

Experts say the Pentagon's smart-card program is probably the world's most complex and far-flung use of smart cards. Analysts say the technology has come at a steep price.

"I don't think it's been as easy to implement as they originally thought," said Brian Ruttenbur, security technology analyst with Morgan Keegan. "I think it's cost a lot more than anticipated."

Ruttenbur estimated the program has cost about \$100 for every desktop computer set up for the cards. He added that ActivCard gets \$8 to \$10 for each workstation.

But Dixon from the Defense Department said the program has stayed within its estimated budget. Up to 2 million desktop computers are set up for the cards.

Ziegel, the analyst who estimated the program has cost up to \$1 billion so far, said the Defense Department has been successful in pioneering the use of smart cards by the U.S. government.

"Its major importance is it's the poster child," he said. "There was some sense of urgency to get these things issued and worry about some of these other potential applications later."

Contact Dan Lee at dlee@mercurynews.com or (408) 920-5425.