SFGate.com Return to regular view
Print This Article

# Passports receiving ID chips
## Infineon gets order for high-tech security documents

- Tom Abate, Chronicle Staff Writer
Tuesday, August 22, 2006

A German semiconductor company with offices in San Jose said Monday that it has received an order from the U.S. government for millions of identification chips that will be embedded in passports to help prevent fraud at border crossings.

Infineon Technologies provided few details about the order. A spokeswoman for the Government Printing Office, which prints and binds passports in Colorado, confirmed the deal.

A French company, Gemalto, has also received an order for a pilot run of the ID chips, she said, but at this point it isn't known whether those will go into volume production.

The chips carry an encrypted digital photograph of the passport holder. The chip is designed to be read by a special device that will be used by U.S. government workers who check passports when travelers come through border crossings.

The State Department began issuing what are being called e-passports to tourists last week and will gradually increase production. State Department spokeswoman Janelle Hironimus said existing passports will remain valid until they expire but, eventually, all U.S. passports -- about 13 million will be issued in 2006 -- will contain such chips.

The decision to mass produce these chip-powered passports comes after a lengthy process during which privacy activists argued that the new electronic devices might give hackers access to personal information. And while their complaints prompted features to boost privacy, skeptics remain.

"Whether the changes are enough, we'll have to find out," said Lillie Coney, associate director of the Electronic Privacy Information Center in Washington.

Jeorg Borchert, a vice president with Infineon Technologies North America in San Jose, said that among other changes made to assuage privacy concerns, the chip-bearing passports will have a foil wrapping inside their covers to prevent the chip from being read electronically while the passport is closed.

Borchert said the protections in the system make it different and far more secure than other forms of radio frequency identification devices that can be read from as far away as 30 feet.

He said the e-passports must be brought within 3 inches of a radio-frequency identification device that works in combination with other security features to prevent unauthorized peeking into the chip.

Development of electronic passports began several years ago, before the current U.S. emphasis on fighting terrorism, under the auspices of the International Civil Aviation Organization. Created at the end of World War II and based in Montreal, the organization helps set standards for air travel.

Interest in e-passports was heightened by the Sept. 11, 2001, terrorist attacks, and in 2002 the United States began moving toward including this sort of electronic verification in passports. "The idea is to make sure the person who is carrying the passport is the person to whom the passport was issued," said Hironimus, the State Department spokeswoman.

But the effort has met with some derision in technical quarters. German security consultant Lukas Grunwald cloned, or copied, the data on an e-passport chip at the Black Hat security conference in Las Vegas earlier this month. "This whole passport design is totally brain damaged," Grunwald told the Web site Wired News.

But State Department officials called it a meaningless stunt because the chip was designed to work in conjunction with other identification features that would thwart any attempt to falsify a passport simply by slipping in a copied chip.

And Grunwald told Wired News that, so far as he can tell, there's no way to alter the encrypted data on the chip without being detected.

*E-mail Tom Abate at tabate@ sfchronicle.com.*

Page E - 1
URL: http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/08/22/BUG2SKMIJ91.DTL