

ELECTRONIC PASSPORTS SET TO THAWRT FORGERS

By Roger Yu, USA TODAY
August 10, 2005

The U.S. passport is joining the digital age. After three years of research and discussion, the State Department has finalized most of the technical and logistical details of new, supposedly tamper-proof passports embedded with a "smart-card" chip.

If current plans hold, they'll become standard issue for U.S. travelers as soon as February.

Proponents say the chip, which will contain the holder's personal data and digital photo, should allow speedier entry at borders for most travelers.

Because the chip's data can't be altered, proponents say, forging passports will be virtually impossible. That, they say, gives authorities a potent new anti-terrorism weapon.

When swiped across an electronic reader, the chip in the passport wirelessly transmits data to a customs officer's computer screen. The e-passport relies on radio frequency identification technology (RFID).

The new passport looks much like the traditional type. But the smart-card chip, embedded in the back page, makes it slightly thicker. If the chip is broken or malfunctions, the holder can continue to use the passport as a non-electronic passport, or buy a new one.

Once the new version is available, it would take up to a year for all new passports to be issued in the new format. Americans with valid traditional passports won't have to replace them until they expire.

The new passport will cost \$97, or \$12 more than the traditional version.

Initially, U.S. diplomats will use the e-passport as a test, probably starting in December, says Frank Moss, deputy assistant secretary of State. If successful, the new passport will be available to the public next year, possibly as early as February, Moss says.

Calls for better border security

The Sept. 11 terrorist attacks prompted calls for improved border security. The new e-passport is perhaps the most visible aspect of the government's foray into digital technology for border control.

The e-passport has raised concerns among critics who say it lacks adequate privacy safeguards. Wireless transmission of data compromises security, and important personal data could fall into the wrong hands, they say. With proper equipment, someone could remotely intercept personal data, they say.

Wireless transmission could lead to what's called "skimming" or "eavesdropping," says Cedric Laurant of the Electronic Privacy Information Center, a Washington, D.C.-based advocacy group.

In skimming, an intruder secretly uses a device to read the chip's data from as far away as several feet.

Americans walking with their passports could be essentially broadcasting their nationality and other personal information, Laurant says.

Eavesdropping could occur at border checkpoints if someone intercepts the information as it's being transmitted from the chip to a reader.

Moss says those concerns are outdated. The agency has made technical adjustments to address them. The State Department has added a metallic anti-skimming material to the passport's cover and spine. It limits retrieval of the data to within an inch of the passport, Moss says.

The State Department is also considering adding a layer of protection by encrypting the information so it can be read only by authorized devices, Moss says.

Bernard Bailey, CEO of software developer Viisage, which is working with the State Department, says e-passport's technology is sound. It will improve national security while safeguarding traveler privacy, he says.

E-passport roots

Bill Connors, executive director of corporate-travel advocate the National Business Travel Association, says the government has adequately addressed the privacy concerns of his organization.

"We feel that the passports are much more secure now," Connors says.

The e-passport initiative has its roots in legislation passed by Congress in May 2002 to improve border security. It called for 27 countries whose citizens don't need visas for entry into the USA to convert to electronic passports by October 2004. Congress has since delayed the deadline until October 2006.

The International Civil Aviation Organization, an international agency, created the technical specifications for e-passports worldwide, and that has helped to enhance international cooperation, says Paul Beverly of smart-card-maker Axalto.

All e-passports will have the same underlying technology and will work with other countries' readers, Beverly says.

If the U.S. meets its target dates for the e-passport introduction, it will be one of the first countries to use it, he says.

Beverly says he's consulted with 20 governments about the chip technology and hasn't witnessed backlash from U.S. demands for a system of electronic passports.

"There were some concerns about the very aggressive schedule, but that objection has largely gone away," he says.