

United States Sets Date for E-Passports

The U.S. State Department says all U.S. passports issued starting in October 2006 will contain RFID chips.

By Paul Prince

Oct. 25, 2005—The U.S. State Department issued its final rules today specifying its plans to issue electronic passports (e-passports) containing RFID tags. The department says it intends to begin its e-passport program in December. The first stage will be a pilot program in which e-passports will be issued to government employees using official or diplomatic passports for government travel. This pilot, the department says, will permit field-testing prior to the first issuance to the American traveling public, early next year. By October 2006, all U.S. passports, with the exception of a small number of emergency passports issued by U.S. embassies or consulates, will contain RFID tags.

The final rule incorporates amendments resulting from comments to a proposed rule originally published in the Federal Register on Feb. 18. The State Department says it received a total of 2,335 comments regarding its proposal to introduce e-passports. The department categorized 98.5 percent of the comments as negative, 1 percent as positive and 0.5 percent as neutral. Regarding issues raised by those comments, the department says 2,019 expressed security and/or privacy concerns; 171 raised general objections to the use of the data chip and/or RFID; 85 expressed general objections to the use of electronic passports; 52 listed general technology concerns; and 8 focused on religious issues. The comments are available for review at the travel.state.gov section of the department's Web site.

The chip used in the e-passports will comply with the ISO 14443 RFID specification and contain the same information as a passport's data page—the passport holder's name, nationality, gender, date of birth, place of birth and digitized photo. The chip will also contain the passport number, issue date, expiration date and type of passport. The ISO 14443 specification permits chips to be read when an e-passport is placed within approximately 10 centimeters of an RFID interrogator (reader).

Of all objections the department received regarding its plans, the overwhelming majority expressed concern over the potential for skimming and/or eavesdropping. Skimming is the act of creating an unauthorized connection with an RFID tag in order to gain access to its data. Eavesdropping is the interception of the electronic communication session between an RFID tag and an authorized reader.

To prevent skimming, the department will add shielding material to the passport's front cover and spine. The material is supposed to make the e-passport's RFID tag unreadable as long as its cover is closed or nearly closed. The department will also implement Basic Access Control (BAC), which functions as a Personal Identification Number (PIN) in the form of characters printed on the passport data page. Before a passport's tag can be read, this PIN must be inputted into an RFID reader. The BAC also enables the encryption of any communication between the chip and interrogator.

To ensure that U.S. e-passports are interoperable with other nations' systems, the document's embedded RFID chip will comply with specifications developed by the International Civil Aviation Organization (ICAO). The

ICAO specification requires a minimum capacity of 32 kilobytes of memory for storing data on the chip, whereas the U.S. government has opted for a chip with 64 kilobytes of memory to allow for the potential storage of additional data or biometric indicators such as fingerprints or iris scans, sometime in the future. Before the department adds additional data or biometric identifier other than a digitized photograph, however, it says it will seek public comment through a new rule-making process.

Several other nations have already begun issuing e-passports, including Sweden (see [Sweden Switches to E-Passports](#)).

Copyright ©2005 RFID Journal, Inc. All Rights Reserved