

# DHS Testing E-Passports in San Francisco

Singapore and Australia airports are also participating in the U.S. Department of Homeland Security's assessment of RFID technology.

By Mary Catherine O'Connor

Jan. 18, 2006—At San Francisco International Airport (SFO), the Department of Homeland Security (DHS) has begun a three-month trial to test the RFID technology underlying electronic passports (e-passports). The documents, which contain RFID inlays encoded with biographic and biometric information about the passport holders, are designed in compliance with International Civil Aviation Organization (ICAO) standards.

The goal of the test is to assess how the RFID interrogators (readers) and biometric equipment needed to process the e-passports will impact the passport inspection process, as well as how well the RFID interrogators read the tags embedded in the passports. It will also gather information supporting other countries' development and implementation of e-passports that comply with ICAO standards.

The number of passports tested during the trial will depend on how many e-passport holders travel through SFO and the two other airports participating in the trial: Changi Airport in Singapore and Australia's Sydney Airport. Any of the roughly 200,000 citizens from Australia and New Zealand who have been issued electronic passports and are traveling through these three airports would participate. The same goes for any Singapore Airlines crewmembers who have been issued e-passports from Singapore (the country has issued approximately 2,000 thus far, specifically for the trial). U.S. diplomats and officials who had been issued electronic passports would also participate.

As of October, all U.S. passports will be issued as e-passports (see United States Sets Date for E-Passports). The U.S. State Department decided to begin issuing e-passports in the hope of making passports more secure documents and harder to counterfeit, as well as expediting passport inspection agents' verification process.

The State Department has received more than 2,000 comments in response to its proposal to embed RFID tags into passports. Nearly all of them were written in opposition to the practice, listing specific concerns over the security of the data encoded to the tags, and the personal privacy of citizens carrying them.

To address these concerns, the government added a security feature known as Basic Access Control (BAC) to its e-passport design. BAC is intended to prevent the unauthorized reading, or "skimming," of information from e-passports. It uses a personal identification number that must be sent to an RFID interrogator before it can access the data encoded on an e-passport's tag.

Also encoded on that tag is a digital image of the passport holder, which can be compared with the person's face during the inspection process, using biometric comparison technology. This will ensure that the image saved to the e-passport matches that of the person presenting it.

The test, which began Jan. 15 and will run until April 15, is the DHS's second. Its first test of the technology took place last year in Los Angeles International airport (LAX) from June 15 to Sept. 15, and was conducted

to support efforts to develop and implement e-passports compliant with ICAO standards. Participants in the LAX test were limited to crewmembers of Air New Zealand, Qantas and United Airlines who had been issued e-passports which were recalled once the tests were complete. BAC functionality was not tested in the LAX tests.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved