

Raytheon Unveils ID Card, Fortifying RFID With Biometrics

The company believes its PAD card, which incorporates a fingerprint scanner for authentication, is well suited for use for the RFID-enabled passport card proposed by the U.S. Departments of Homeland Security and State.

By Mary Catherine O'Connor

Feb. 13, 2007—The Intelligence and Information Systems business division of government defense, aviation and technology company Raytheon has unveiled a new RFID-based identification card. Dubbed the PAD—which stands for personal authentication device—this card incorporates a fingerprint biometric authentication function. The company is pitching the PAD for use in border security programs run by both the Department of Homeland Security (DHS) and the Department of State.

Raytheon believes the PAD is particularly fitting for use as the proposed RFID-enabled passport card, part of the PASS (People Access Security Service) system introduced last year by DHS Secretary Michael Chertoff. The intended purpose of the PASS card—which would be used instead of a passport for land or sea travel in the Western Hemisphere—is to improve border security while also facilitating the flow of legitimate travel and trade over U.S. borders (see DHS Proposes Vicinity RFID Technology for Passport Card). The agencies' plan is to embed passive EPC Gen 2 RFID tags in the passport card that conform to the ISO 18000 6-C specification and have a read range up to 20 feet. However, after receiving a number of public comments opposing this plan, they extended the public comment period from its original Dec. 18, 2006, end date to Jan. 8, 2007 (see DHS Privacy Committee Finalizes Report on RFID IDs).

The government is still reviewing comments and has not yet announced its next step. Many complaints came from vendors of high-frequency RFID technology, who claim UHF technology is inappropriate because UHF's long read range would make the card vulnerable to skimming (the surreptitious reading of a tag by an unauthorized third party) or eavesdropping (the unauthorized interception of RF transmissions between a card and reader). The shorter read range and data encryption tools available with high- or low-frequency inlays, UHF's critics say, would protect against these vulnerabilities.

Guy Swope, Raytheon's senior biometrics architect, says the PAD could support data encryption for the UHF EPC Gen 2/ISO 18000-6C inlay inside the PAD. While Gen 2 chips do not offer enough processing power to support the most widely used means of data encryption (which are used for protecting data encoded to ISO 14443 and ISO 15693 HF inlays), the processor used to perform the biometric matching provides enough memory for tag data encryption. However, Swope notes, Raytheon is only interested in deploying a data encryption process that is viewed as an industry standard, and no such process has yet been identified for Gen 2 tags.

The front face of the PAD, which is roughly the size of a credit card, could be printed with information about the cardholder, such name and birth date, along with a photograph. In the middle of the card would be a small fingerprint scanner. To authenticate that the rightful owner is presenting the ID, the cardholder would press a

thumb onto the fingerprint scanner while using another finger to press an on/off switch on the back of the card to engage the battery required to operate it.

Thus far, Raytheon has mocked up the PAD into a small number of prototypes. Swope notes that his firm has built some flexibility into the final design, enabling end users to deploy the PAD card slightly differently if they preferred. For example, the on/off switch powering the fingerprint scanner could also act as a means of making the tag inside the card unreadable when unpressed. It would do this by acting as a switch that disconnects the tag's antenna from the chip unless the switch is pressed.

The PAD contains a memory chip on which the traveler's thumbprint scan is saved at the time of issuance. Also embedded in the PAD are red and green LEDs for indicating whether the scans match.

Swope says that the PAD card would fill in some holes in the current passport card proposal. For example, the proposal does not call for a biometric authentication tool. Thus, Swope says, "[border patrol] will know that the card has left the country, but not the person." By combining RFID and biometrics, he adds, the PAD can ensure both.

According to Swope, Raytheon envisions the border patrol using the PAD card to authenticate travelers on foot or by vehicle (air travel across U.S. borders requires the use of a passport). Travelers crossing a border on foot would stop at a prescreening station prior to approaching a border patrol agent. A traveler would hold the PAD in front of an RFID interrogator at the station and activate it by placing a thumb on the scanner and pressing the on/off switch. If the traveler's thumbprint matched the one saved in the PAD's memory, a green light would flash on the card's face. If it didn't match, a red light would flash.

In either case, the positive or negative result, plus the PAD's unique ID number, would be captured by the RFID interrogator and transmitted to back-end software, then sent to the border agent's computer terminal. When the traveler reached the agent, he or she would do a secondary, visual check of the traveler if the result registered a match. If it failed to match, the traveler would go to another area for secondary screening.

RELATED_ARTICLES The scenario for use at a vehicle crossing would be much the same, except that the vehicle passengers would use the PAD to scan their thumbs while driving through an RFID-enabled portal leading up to a border patrol agent's gate. Swope says Raytheon has confirmed that the portal can read the card number and thumbprint scan from a vehicle moving as fast as 60 miles per hour. The vehicle would then have to stop at a border patrol gate so an agent could make a secondary visual check or direct the vehicle for secondary screening, if needed.

Raytheon has a large number of contracts with the U.S. government, and Swope says the company has been in discussions with DHS representatives regarding the use of PAD for the PASS card and other applications. However, he will not provide details outside of saying that the discussions are "going well." He also declines to name the manufacturer of the PAD card's tag. Outside of government applications, he says, the PAD card could be used in the private sector for building security.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved