

# RFID Vendors Brief Congress on PASS Card Security

During a meeting with congressional aides, industry representatives explained why they believe the proposed use of EPC UHF Gen 2 tags in the ID cards is problematic.

By Mary Catherine O'Connor

July 20, 2007—During a congressional briefing in Washington, D.C., on Wednesday, security and privacy advocacy groups and RFID vendors criticized the [U.S. Department of Homeland Security's](#) decision to use EPC UHF Gen 2 tags in IDs being developed as part of the Western Hemisphere Travel Initiative (WHTI).

"We have a situation where the government is issuing [identity] cards to themselves that are more secure than what they are about to issue to the citizens. There is something significantly wrong with the situation," said Neville Pattinson, vice president of government affairs and standards at [Gemalto](#), a digital security company based in Amsterdam.

Pattinson was addressing the 50 congressional staffers, government officials and industry representatives attending the briefing. Sponsored by security and identification industry groups [SecureID Coalition](#) and [Smart Card Alliance](#), the briefing was intended to provide an overview of best practices for securing electronic identity credentials used in federal programs.

Pattinson, who sits on the DHS' Data Privacy and Integrity Advisory Committee, was referring to the so-called Common Access Card issued by the [U.S. Department of Defense](#) (DOD) and used by 12 million active-duty military, other DOD personnel and DOD contractors for access to Department of Defense facilities and computer systems. He contrasted the DOD's card with the proposed PASS (People Access Security Service) card slated to be issued as part of the WHTI, to U.S. citizens making frequent land-border crossings into Canada or Mexico.

Currently, the Common Access Card contains a contact-based embedded computer chip encoded with the bearer's identity information, using data encryption to ensure that the card's data doesn't fall into the wrong hands. Soon, the card is likely to also carry a high-frequency RFID inlay to transmit this encrypted data. The proposed PASS card, on the other hand, would use a standard UHF EPC Gen 2 inlay, which does not support data encryption. As such, the ID number encoded to the PASS card inlay could be easily cloned.

Pattinson urged attendees to question the direction in which government agencies are moving the PASS card. He stated that close-range RFID technology with built-in cryptography—which he, Gemalto and the Smart Card Alliance refer to as "contactless smart-card technology"—would be the only means of ensuring that the PASS card program would be deployed in such a manner as to provide the government with electronically authenticated, forge-proof identity documents, while also protecting the privacy of U.S. citizens by making the encoded data inaccessible to nefarious parties attempting RF-eavesdropping.

Concern over the use of UHF EPC inlays in PASS cards has led to an extension of the public comment period

on the proposed card, which closed in January of this year. The Bush Administration conceived of the card as a cheaper alternative to U.S. passports for citizens making frequent land border crossings, and directed the DHS to implement the program under the Western Hemisphere Travel Initiative. The department then charged its U.S. Customs and Border Protection agency with the task of defining the technology to be used in the card. Of the 4,000 public comments the DHS received regarding the proposed PASS card, Pattinson says, all but three expressed opposition to the use of UHF RFID without data encryption. Still, he notes, "[the agencies] are intransigent in considering the alternatives to [using] insecure RFID tags."

However, he adds, Congress is mandating a delay of 18 months to the PASS program because it is unhappy about "DHS rushing to set this up with insecure technology choices." The sponsors of the briefing hope that during this delay, they can convince Congress to call for more trials of the proposed technology before the PASS cards are rolled out to citizens.

James Wiley, director of electronic documents at RFID chip, tag and reader maker Texas Instruments (TI), provided attendees an overview of the best practices his company recommends for the use of RFID in identity documents.

In any identity authentication system deployed by the government, Wiley explained, "there are two players: the citizen, whose identity is being challenged, and the government, who is working to authenticate the citizen. Both groups have serious and legitimate concerns, and any best practices need to address both groups." He added that "Security need not be attained at the price of privacy or operational efficiency," maintaining that clear rules must be set, pertaining both to the procedural and technological aspects of the identification system.

On the procedural side, Wiley stated, the government must inform each citizen, in advance, about which personally identifiable information is being collected, where this data is being collected, how it is being saved and with whom it is being shared. Citizens must also have a means of correcting inaccurate data linked to them through the identification system, and, whenever possible, their participation in the system should be voluntary.

On the technology side, he said, any RF-enabled identity document, and the reader used to collect data from that document, must each be authenticated by the government agency before any data is transmitted between the card and reader, to ensure both elements are legitimate and authorized. Moreover, all data transmitted via RF signals between a card and reader should be encrypted to protect it from being captured by an unauthorized party.

"RFID encompasses an incredibly wide range of technologies, and there are a lot of different flavors of this stuff," Wiley said, pointing in particular to the differences between the high-frequency cryptographically protected RFID inlays used in many identification and payment systems, and the long-range UHF inlays, incapable of supporting data encryption, that the DHS wants to use in the PASS card. TI manufactures both HF inlays that support data encryption and UHF inlays that do not.

**RELATED\_ARTICLES** For the benefit of the attendees, Wiley used a prototype PASS card containing an EPC Gen 2 UHF inlay and an off-the-shelf RFID interrogator to show how simple it is to capture and encode the prototype's identification number onto another EPC inlay. "The attendees were amazed by how quickly and easily the Gen 2 tags could be cloned," says Pattinson.

According to Pattinson, Gemalto and the other companies and groups at the briefing will continue to petition for the establishment of a technology trial in which EPC tags will be tested alongside high-frequency data-encrypted tags and other technologies.

