

Agencies Affirm Privacy Policies for RFID

A panel of government officials explained how agencies are trying to build privacy safeguards into potential U.S.-issued RFID-enabled IDs.

By Elizabeth Wasserman

July 18, 2005—U.S. government agencies are trying to build consumer privacy protections into applications of RFID-based secure microchips being considered for identification purposes, representatives of several agencies said during a panel discussion sponsored by AeA (formerly the American Electronics Association) in Washington, D.C.

Federal agencies are undertaking privacy impact assessments for potential applications of RFID-enabled secure IDs, such as electronic passports (e-passports). In addition, government officials said privacy protections are being considered in the design, introduction and use of these solutions. Required by the E-Government Act of 2002, a privacy impact assessment (PIA) is a procedure designed to make sure that when government agencies develop a new information technology (IT) project or redesign business processes, they consider privacy implications. Each agency carries out its own PIA for RFID-enabled ID applications and publishes the findings.

"We have privacy baked in," said Kenneth Mortensen, an attorney in the U.S. Department of Homeland Security's Privacy Office. The mission of the DHS Privacy Office is to minimize the agency's impact on individual privacy while achieving the goal of strengthening homeland security. The Privacy Office is responsible for ensuring that the DHS complies with federal laws when handling private information, as well as for reviewing regulatory proposals and conducting PIAs for new rules or programs.

The department is shepherding a program called US-VISIT (United States Visitor and Immigrant Status Indicator Technology), an integrated system to record entry into and exit from the United States that will use biometric data to identify aliens and immigrants. That data will be stored on RFID chips attached to arrival and departure forms. A test of the program is expected to begin this August. If successful, the program will reportedly be deployed at the 50 busiest land ports of entry at the nation's borders with Mexico and Canada by December 2007.

Mortensen said the DHS undertook a privacy impact assessment (published in January 2004) for the US-VISIT program, and has been considering privacy implications from its conception. One of the roles of the privacy office, he added, is to work with and question project managers and technologists. "What is the purpose?" he said he asks, and "Why am I using or collecting or storing this information?" He explained that this type of examination often helps project teams understand how to build solutions that protect privacy.

With more than 2,500 member companies, AeA is said to be the largest nonprofit trade association of high-tech companies in the United States. The organization held the panel discussion on Thursday as part of a program to help educate legislators, public policy officials and members of the private sector about issues surrounding deployment of RFID technology. AeA has scheduled a variety of briefings on issues—such as RFID and port security, RFID and homeland security and customs, and RFID and federal

procurement—throughout the rest of 2005.

The panel on privacy implications was held to help correct public misperceptions about RFID technology and confusion between its use in supply chains by companies such as Wal-Mart and Target and its use to secure identifications. "People are scared," said Marc-Anthony Signorino, AeA's director and counsel of technology policy, "because people don't know."

Agency officials invited to the panel discussion on privacy also included Dan Caprio, deputy assistant secretary for technology policy and chief privacy officer at the U.S. Department of Commerce, and Michael Butler, director of smart card programs and operations in the Defense Manpower Data Center, the repository of personnel, training and financial data at the U.S. Department of Defense. Representing the private sector was Joerg Borchert, vice president of chip card and security for chipmaker Infineon Technologies.

One of the federal government's most high-profile uses of RFID technology is in e-passports, which would be issued through the U.S. Department of State. The State Department and the U.S. Government Printing Office have been testing e-passports since last October (see U.S. Tests E-Passports). The department had hoped to begin issuing e-passports to the public in the first quarter of 2005, but in order to address privacy concerns, it delayed introduction until later this year, with full deployment now expected in 2006.

Other agencies, such as the Department of Defense, have already been issuing secure IDs to their own employees. The DOD began its program four years ago. Butler, who runs the program, said employees and unions were initially alarmed at the issuance of the RFID-enabled IDs, but after an education campaign that included details on how the cards use encryption, they started using them with little complaint, he claimed.

Caprio, from the Department of Commerce, which helps other agencies with standards and spectrum issues, noted that many uses of RFID—including the automatic payment of tolls on highways—have gained public acceptance. But tradeoffs occur, involving peoples' decisions to give up some private information for some type of better service, such as not having to wait in line at tollbooths. "This is a gain benefit," Caprio said. "Someone has access to the information, but we have the expectation that they will only use it for toll purposes. We make these mental trades [giving up some private information to get a better service or a discount] all the time when we use grocery cards and loyalty cards."

Copyright ©2005 RFID Journal, Inc. All Rights Reserved