

NIST Completes RFID Security Guidelines

The National Institute of Standards and Technology's report describes the risks to data security and personal privacy that RFID deployments may pose, and provides best practices and procedures to mitigate those dangers.

April 27, 2007—[The National Institute of Standards and Technology](#) (NIST), a non-regulatory agency of the [U.S. Department of Commerce](#) (DOC), released this week its guidelines describing the various risks to data security and personal privacy that RFID deployments may pose, while also providing best practices and procedures, based on existing technology and regulations, to mitigate those risks. The 154-page report, [Guidelines for Securing Radio Frequency Identification \(RFID\) Systems](#), is meant to assist retailers, manufacturers, hospitals, federal agencies and other organizations in understanding how to deploy RFID technology securely and safely.

The paper focuses on RFID applications in the product supply chain, including tracking at the item level, says Tom Karygiannis, senior scientist at NIST and lead author of the paper. It does not address the use of RFID technology in smart-card applications for identification or payments, or applications that use near-field communications (NFC) technology.

The paper opens with an introduction to radio frequency identification and its essential components, and provides an overview of different RFID applications in the supply chain. It also discusses the business risks associated with the technology and the security tools that can be used to mitigate these risks, such as basic IT security measures and encoding policies intended to prevent sensitive data from being encoded directly to RFID tags. Other best practices it recommends include encrypting tag data where and when appropriate; allowing only authenticated parties to access RFID hardware and software systems, taking measures to limit physical access to tags so they can't be cloned or otherwise compromised; and auditing data logs and time-stamping tag-read events to help detect security breaches.

In addition, the report provides an overview of privacy regulations and controls, particularly as they pertain to federal agencies. Privacy was not a focus of the original draft of the report, but the committee revising the paper found it hard to talk about security without discussing that issue, as the two topics are so intertwined.

“This [report] is an example of how the federal government has a role in shaping the future of the market for RFID products, and why it is important for those in the industry to pay attention to, talk to, advise and provide input to folks like those at NIST,” says Douglas Farry, a managing director of international law firm [McKenna, Long & Aldridge](#) and lead correspondent for the [RFID Law Blog](#).

NIST had released a draft of the paper in September (see [NIST Releases RFID Security Recommendations](#)), after which it held a 30-day public review and comment period. “In the first month, there were 50,000 downloads of the draft document [from the NIST Web site],” says Karygiannis. “We received more than 300 comments in total, though some organizations made multiple comments. We received many comments from people who wanted more information on the privacy issue.”

Organizations that commented on the draft include industry group EPCglobal and network infrastructure (and EPC directory) services provider VeriSign, as well as data security providers and representatives from the U.S. Departments of Defense, Health and Human Services, Homeland Security and Labor. According to Karygiannis, some of the questions NIST received were easily addressed in the final report, while others led to revisions in the document's content. "You always learn things from people who are out in the field, rolling up their sleeves," he says. "It's one thing to do a technical analysis [of a given technology] in the lab setting, but another to get feedback from people using the technology."

The paper discusses the Privacy Act of 1974 and the Organization for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which, the report says, "provide a framework for privacy policy that has been referenced in U.S. federal guidance and internationally." It also points to the E-Government Act of 2002, as well as policies from the Office of Management and Budget and guidelines from the Health Insurance Portability and Accountability Act (HIPAA), which describe protections for information related to persons' health.

"At NIST, we don't create regulations or policies," says Karygiannis, "but in the report, we point to the existing regulations that someone at an organization that is charged with writing a privacy policy regarding RFID should consider."

Among the recommended practices for organizations deploying RFID, the paper describes a five-phase life cycle to help determine the most appropriate actions to take at each point in the development of an RFID system. The life cycle is based on a model introduced in NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle. In Phase One, Initiation, it suggests that organizations perform a security and privacy risk assessment and develop policy and requirements with which the RFID system must comply.

In Phase Two, Acquisition/Development, the report says RFID network architects should specify the security requirements with which the RFID system must comply, as well as how the hardware and software to be deployed will support these criteria. In Phase Three, Implementation, it reads, "procured equipment is configured to meet operational and security requirements, RFID data is integrated with legacy enterprise systems, and staff are trained in the proper use and maintenance of the system." For Phase Four, Operations/Maintenance, the organization deploying RFID performs such security-related tasks as periodic security assessments, applying security-related software patches and reviewing RFID event logs. And during Phase Five, Disposition, several security steps are outlined, such as preserving information to meet legal requirements, and disabling or destroying tags and other components when they are taken out of service.

To illustrate how these best practices and five-phase life cycle can be deployed, the report includes two hypothetical case studies—one regarding a personnel- and asset-tracking application in a health-care setting, the other involving the management of hazardous wastes—to illustrate how RFID security might be implemented in practice.

RELATED_ARTICLES Patrick Sweeney, CEO of RFID systems integration firm ODIN Technologies, says the report shows RFID technology can be deployed securely. "The key take-away is that the security of RFID requires a very specialized level of understanding, expertise and process," he says. Sweeney will appear along with RFID end user Shaw Industries and Robert Cresanti, the DOC's undersecretary of commerce and technology, at next week's RFID Journal LIVE! 2007 conference in Orlando, Fla. In a prepared statement, Cresanti noted that the NIST report "lays the foundation for addressing potential RFID security risks so that a thoughtful enterprise can launch a smart tag program with confidence."

The full NIST report is available for download at http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf.

