THE RFID DEBATES

Nov 1, 2005 12:00 PM, By Michael Fickes

Smart cards have transformed access control and ID badging into technologies so powerful that the government — at least in California — has taken notice and moved to regulate their use in public applications. The contactless smart card industry is fighting the effort.

Since the regulatory focus thus far has aimed at public or government applications, corporate security directors may assume the debate does not concern private sector uses of radio frequency identification (RFID) technologies. In fact, the debate between the California legislature and the smart card industry may eventually define — if not legislate — acceptable and unacceptable uses for RFID-enabled contactless smart cards in private and public venues. The debate has certainly shown that the public is vitally interested in the privacy issues raised by RFID technology.

Here's how the argument started. Back in January, the Brittan Elementary School in California's Silicon Valley announced that school officials had decided to switch to a new student ID badge. Five days later, children came home from school wearing breakaway lanyards designed to hold the new badge with a 5×4-inch plastic device with a radio frequency (RF) transmitter attached to the back. At first, parents did not know what the transmitter was. Once it was identified, however, it worried them. Could an unauthorized person intercept the signal being sent out and track children? Should school officials employ technology to track children? Is it ethical? How might this technology be misused? Should government regulate its use?

Industry observers say that the school's effort was misconceived from the beginning. The children were given active RFID tags. Quite different from relatively secure passive smart cards, active RFID tags broadcast data constantly to receivers as far away as a few hundred feet.

Parents objected, filed complaints with the district and spoke to their state government representatives. Senator Joseph Simitian, a Silicon Valley lawmaker recognized for his knowledge of technology, took up the cause and introduced legislation designed to control the use of RFID technology in identity management and access control applications by state and local governments in California. Earlier this year, the State Senate passed the Identity Information Protection Act of 2005 by a lopsided and bi-partisan vote of 29-7. The State Assembly — the lower house in California government — will begin its consideration of the bill shortly.

According to Simitian, the bill, as it is now written, would do three things:

make the unauthorized reception of information from RF identification devices a crime;

require privacy protections for RF identification devices, including the use of a unique identifier, encryption and authentication protocols; and

set up a three-year moratorium on government mass distribution documents with RF identification capabilities.

Industry objections

The smart card industry has mounted a vigorous attack on the bill. In response to the bill's first goal of criminalizing the unauthorized skimming of RF information from smart cards, Daniel Greenwood, an industry consultant and advisor as well as an attorney specializing in e-commerce and security, notes that a California computer crime statute already prevents unauthorized access to computer systems.

Are smart cards computer systems? Smart card microprocessors probably qualify as computer systems, Greenwood says. He contends