

## New Coalition Will Confront RFID Security Hype

Wednesday August 16th, 2006

A handful of chip makers and smart card producers have come together and formed the Secure ID Coalition with the goal of promoting smart card technology while simultaneously ensuring consumer privacy and data security. Chip makers Texas Instruments, Philips Semiconductors, and Infineon Technologies, along with smart card makers Gemalto and Oberthur Card Systems announced their founding of the organization at this week's National Conference of State Legislators in Nashville, Tennessee.

The idea behind the coalition was the need to better confront the seemingly endless -- and often baseless -- pronouncements about RFID and smart card security vulnerabilities. The most recent example is the copying of e-passport data by security consultant Lukas Grunwald, which made headlines across the technology press despite industry experts dismissing it as a total non-finding (see [New RFID Passport Scare -- Does it Matter?](#)). Another example was the study published in March by researchers at Vrije Universiteit in Amsterdam which asserted that RFID tags could carry malicious code to infect computer systems with which they came in contact (see [Study: RFID Vulnerable to Viruses and Worms](#)). That study also received widespread attention but was ultimately derided by experts as contrived and extremely unrealistic (see [The Industry Reacts to RFID Virus Research](#)).

There are two issues that the Secure ID Coalition seeks to address. The first is simply to offer a response system. If, as in the case of last week's e-passport "hack", the announcement is found to be hyped or the threat exaggerated, the Secure ID Coalition will act as a resource for press, analysts, and legislators to better understand the issue. The second is helping distinguish between RFID and smart cards, which, while related, are not the same technology. Tres Wiley, manager of e-documents for Texas Instruments, said that the conclusions of many of the security analyses often "mix apples and oranges" by lumping smart cards in with RFID. Smart card technology is not particularly new, and its

## Free, sign up now!

Sign up below to receive RFID news regularly in your inbox. Fields marked \* are required.

|                    |   |
|--------------------|---|
| First name: *      | <input type="text"/>                          |
| Last name: *       | <input type="text"/>                          |
| Email address: *   | <input type="text"/>                          |
| Confirm email: *   | <input type="text"/>                          |
| Company:           | <input type="text"/>                          |
| Address 1: *       | <input type="text"/>                          |
| Address 2:         | <input type="text"/>                          |
| City:              | <input type="text"/>                          |
| State:             | <input type="text"/>                          |
| Zip/postal code: * | <input type="text"/>                          |
| Country: *         | <input type="text" value="Please select..."/> |
| Industry: *        | <input type="text" value="Please select..."/> |
| Job function: *    | <input type="text" value="Please select..."/> |

[RFID Talk](#) is the RFID industry's leading discussion forum. Choose a username and password below if you would like to join.

|               |                      |
|---------------|----------------------|
| Username:     | <input type="text"/> |
| Password:     | <input type="text"/> |
| Confirm pass: | <input type="text"/> |

[Subscribe to RFID Update »](#)

security capabilities have only come under the spotlight as security specialists and hackers have recently turned their focus to RFID.

"The [smart card] technology has been under development for years. It's thoroughly vetted, with very few issues with standards, and a broad array of vendors. Overall it's a well-established technology," said Wiley. "We don't want the years of that hard work to be undermined by some of the new applications," referring to RFID's adoption across retail and the supply chain and the resulting interest from hackers.


One of the coalition's responsibilities will be education, for both legislators and end users. With respect to legislators, the coalition doesn't want to see laws hastily enacted as a rash overreaction to fluke occurrences. Such was the case in California, where state senator Joe Simitian introduced broad legislation to curb the use of RFID in identification documents. The legislation was largely in response to the student-tracking fiasco that occurred early last year at an elementary school in Sutter, California (see [Uproar Over School's RFID Student Tracking](#)). "The more we educate people and show them the facts," said Wiley, "the easier it is for them to come to a rational decision about what should and shouldn't be done [with respect to smart card legislation]."

Lastly, the coalition will encourage best practices to implementers of smart card systems, said Jim Sheire, manager of government programs for Philips Semiconductors. He explained that the prevention of hacking relies not just on the security of smart cards themselves, but also on the systems implementation. "We want to make certain that systems that are implemented are implemented correctly," he said. "Clearly the failure of a system could do irreparable damage [to public perception of smart cards]."

Read the [announcement](#)

---

[Home](#) | [Archives](#) | [Forums](#) | [Marketplace](#) | [Subscribe Free](#)  
[About](#) | [Advertise](#) | [Contact](#) | [Contributors](#) | [Privacy Policy](#)

Read *RFID Update* in your favorite news reader: 

© 2006 ALX Technologies