

Calif. Bill Allows RFID in More IDs

Modification to the state's proposed Identity Information Protection Act would permit RFID tags in many government-issued ID documents, provided certain conditions were met.

By Mary Catherine O'Connor

June 24, 2005—After a series of meetings with representatives of The High-Tech Trust Coalition, an RFID industry group that opposes California's proposed Identity Information Protection Act, Senator Joe Simitian (D-Palo Alto) revised the bill that he originally authored. The revisions to the act, known as [Senate Bill \(SB\) 682](#), would allow the use of RFID technology in some identification documents issued by the state or local governments if specific security controls are applied to the RFID chip used in the documents to safeguard it from being surreptitiously read. However, because the act still prohibits the use of RFID (what it calls contactless integrated circuits) in driver's licenses, student IDs, government health and benefit cards and public library cards, the industry coalition is still voicing strong opposition to the act.

Simitian introduced the bill to the state senate in February, and it was approved by a vote of 29 to 7 on May 16 (see [Calif. Senate Approves RFID Bill](#)). It was then sent on to the state assembly for a June 21 hearing. Last week, however, Simitian introduced an amended version of the bill, and the chairman of the state assembly's judiciary committee asked for more time to review it. The hearing by the entire assembly has since been rescheduled for July 28.

The coalition that prompted the bill's revisions says that by using protective measures such as data encryption and mutual authentication between the document and reader (also known as an interrogator), identity documents would be more protected from tampering, forgery and ID theft than they would be without using RFID. The senator asserts, however, that the protective measures thus far developed for contactless ICs would need to be proven more widely effective before they could be trusted to protect information on IDs such as driver's licenses, which are distributed on such a massive scale and read by such a large number of agencies and businesses.

"The industry would be well advised to take a long view of this," says the senator. If security measures failed and sensitive information on California citizens fell into the wrong hands, or was read without a document owner's consent or knowledge, he explains, "it could really set back the technology."

The High-Tech Trust Coalition drafted a two-page letter to the senator detailing its opposition. The coalition claims the bill is poorly drafted and ignores "internationally accepted general security standards," including the Federal Information Processing Standard and ISO 14443, that were designed to protect data transmitted by contactless ICs. The letter is signed by more than 25 companies and organizations, including the [Association for Automatic Identification and Mobility](#), the [California Chamber of Commerce](#), [EDS](#), [EPCglobal](#), [Oracle](#), [Philips Semiconductors](#), [Symbol Technologies](#) and [Texas Instruments](#).

Members of the coalition, including French smart card manufacturer [Oberthur Card Systems](#); the nonprofit trade organization [American Electronics Association](#), based in Santa Clara, Calif., and Washington, D.C.; contactless smart card and interrogator manufacturer [HID Corp.](#), based in Irvine, Calif.; and German

chipmaker Infineon, met with the senator on three occasions after the senate passed the bill. In addition, Oberthur states, the coalition sent a lobbyist to talk to Senator Simitian prior to the bill's passage.

"I've seen some moves by the senator to turn the focus on privacy [protection] rather than the technology," says Patrick Hearn, who attended two of the meetings and is Oberthur's government and ID business development director. "But the way we understand it, the focus is still to ban the technology. My view is that this bill should be defeated. SB 682 is a reactive and overly broad piece of legislation focused on technology instead of bad behavior."

Hearn says the coalition met with the senator on May 18, two days after the senate passed the bill, to discuss how encryption methods, ISO standards and existing laws could be used to protect documents. It met with him again during the last week in May to discuss more technical details surrounding the technology and what would be required to skim information from documents carrying tags with security protections. It then met with Simitian on June 8 to propose that the bill be amended with a three-tiered approach in which documents requiring the most security, such as driver's licenses, would be issued the strongest data protections through data encryption and authentication tools. The second and third tiers would include documents such as library cards and identification badges for accessing buildings, and would have progressively fewer security protections.

The group argued that this approach would ensure that the most sensitive documents would be protected, and would also allow RFID to be used with less privacy-sensitive documents without being cost-prohibitive to deploy.

"I've offered substantial amendments [to the bill] in response to industry concerns," says Simitian, "and I find it regrettable that the more accommodations I make, the more opposition I seem to draw."

On June 15, Simitian submitted the amended version of SB 682. He says amendments turn the bill on its head. Where it once strictly prohibited the use of contactless integrated circuits, for instance, it now permits that use but only with safeguards.

"I wish that industry would recognize the legitimate concerns that the public has about this technology," he said, referring to the use of radio waves to broadcast data.

The bill lists the security measures that must be used to protect the government-issued identity documents it now says can employ RFID. The document's RFID tag must not transmit anything other than a unique ID number. Encryption must be used to protect the data on the RFID chip from unauthorized reading. The reader and document's chip must use mutual authentication. The ID holder must authorize the reading of the ID's data and be notified in writing that the ID uses RF to transmit information, and that he or she can use a shield to prevent the data from being transmitted through RF. In addition, the ID holder must be informed of the locations of all devices intended for use in reading the ID.

SB 682 still allows the use of RFID in identity documents for California's corrections system, emergency first responders, state-run medical facilities, state-run door access cards and automatic toll-bridge collection systems, exempting them from having to meet most or all of the security protections mentioned above. The bill also exempts all systems currently in use by state, county and municipal governments from the provisions of the bill.