News Bulletins

Vendors Form Group To Counter U.S. Privacy Concerns

Five smart card industry vendors have formed an interest group to counter the increasing flow of stories in the mainstream press in the United States questioning the security and privacy of chip-based ID documents.

Card makers Gemalto and Oberthur Card Systems and chip manufacturers Infineon Technologies, Philips Semiconductors and Texas Instruments are scheduled to announce today the formation of the "SecureID Coalition," which will seek to "promote the understanding and appropriate use of smart card technology" and how the technology can help in "maintaining user privacy." The founding members, most based in Europe but which have significant U.S. operations, were to announce the new group today during the first day of the meeting of the National Conference of State Legislators, which represents lawmakers from the 50 U.S. states. The gathering is in Nashville, Tenn.

"We've seen a lot of confusion, in particular with the contactless technologies, over security and privacy concerns," Tres Wiley, director of eDocuments at Texas Instruments, tells *Card Technology*. "There's a lot of misinformation going on out there."

Wiley says vendors formed the group specifically in response to a proposed law in California barring use of contactless or RFID chips in government-issued ID documents and a controversial border-crossing card planned by the U.S. Department of Homeland Security as part of the federal government's Western Hemisphere Travel Initiative.

But even as the coalition was being announced, bad publicity continued over a demonstration at a security conference earlier this month in Las Vegas of the cloning of a German electronic passport. Lukas Grunwald, founder of Germany-based consulting firm DN-Systems, conducted the demo and has been quoted in articles saying data in the e-passport chips is easy to copy and that the "whole passport design is totally brain damaged."

While another U.S.-based vendor group, the Smart Card Alliance, refuted the security and privacy threats, press reports of the cloning attack continue to put passport officials on the defensive.

"All he (Grunwald) appears to have done is follow the (electronic passport) specifications to be able to read the e-passport like any border security agent," says Neville Pattinson, director of marketing and government affairs at Gemalto. He noted what press accounts usually don't say is encryption technology that is part of the global e-passport program would "lock all of the data" on the chip together. It means that while a counterfeiter could clone the data onto another chip and embed it into a fake passport, he couldn't change any of the data, including the digital

photo. If someone tried to use the phony passport, the photo appearing on the border-control agent's screen would not match that of the person presenting the document. The clone, therefore, would only work at unmanned border checkpoints without active biometric systems.

Counterfeiters or others with ill intent also would not be able to skim or eavesdrop the data using a concealed antenna and reader because of a separate security feature, basic access control, or BAC, which requires the e-passport be opened and a code scanned on the data page before the contents of the chip could be accessed. This security feature also encrypts the data passing between passport and reader, says Pattinson.

A separate copper shield the U.S. State Department is including on its e-passports is also designed to thwart any attempts to steal chip data from unsuspecting citizens, although vendors say the shield probably isn't necessary along with BAC.

But the State Department had been slow to add the extra security features compared with more privacy-conscious European governments, which planned to support BAC in their e-passports early on. Privacy advocates in the United States seized on the lapse and the resulting press articles no doubt have contributed to an overall anxiety many U.S. citizens and consumers feel over smart card technology–not only in e-passports, but ID cards and contactless payment cards.

Vendors say they need a new organization to educate and lobby policymakers and journalists to clear the path for the e-passport rollouts, which have begun, and for future ID programs–from chip-based ID cards for government employees to driver's licenses that may carry chips.

"Some of the pain we've gone through with the passport program, we don't want to go through with other programs," says Texas Instruments' Wiley.

In general, privacy groups and the mainstream press are confusing RFID chips like those used for inventory tags with more secure contactless chips, say the vendors.

"This is one of our missions, to clarify and dismiss some of the exaggerated, often inaccurate, statements of privacy advocates," says Pattinson.

The coalition plans to confine its activities to the United States. From the increasing intensity of the debate there over the security and privacy protections afforded by the new generation of ID documents, the new vendor group may have its work cut out for it.

For example, one of the largest privacy groups opposing many of the new types of ID documents is the American Civil Liberties Union. In a letter late last month to the Department of Homeland Security's Privacy Office, it blasted all uses of RFID or contactless technology for identifying people because it could allow for tracking of individuals and increase the risk of identity theft. The advocacy group doesn't appear satisfied with the extra security and privacy measures the State Department has added to the U.S. e-passports.

"Most security countermeasures, such as encryption, mutual

authentication, basic access control and shield devices have never been deployed together in a mass contactless ID system," the ACLU said in the letter. "Their effectiveness has not withstood the test of a real-world deployment; therefore, the government should expect that some method for circumventing these protections could and will be devised." (2006-08-16)