

Industry Group Says E-Passport Clone Poses Little Risk

Cloning a passport's inlay, according to the Smart Card Alliance, would be no different than stealing someone else's passport and trying to present that as your own at a border entry point.

By Mary Catherine O'Connor

Aug. 9, 2006—At last week's [Black Hat](#) computer security conference in Las Vegas, Lukas Grunwald, a consultant with computer security firm [DN-Systems](#), demonstrated that using an open source software package called RFDump and an RFID interrogator (reader), he could duplicate the data from his RFID-enabled German passport onto an RFID access card. With the United States soon to join the handful of nations already issuing passports with embedded RFID tags (the U.S. State Department plans to begin issuing e-passports on Monday), the demo struck a nerve. At last count, a search on [Google](#) showed a few hundred news stories about the event.

One of these stories, published in [Wired News](#), said that to read the tag in his passport, Grunwald used the same interrogator that border agents use to read e-passports and e-passport software made by [Secunet Security Networks](#). He then used RFDump to make the clone.

However, Grunwald merely cloned the data on the IC inside his passport. He did not counterfeit the passport, nor did he manipulate the data. Although Grunwald claimed to have demonstrated a fundamental security flaw in RFID-enabled passports (known as e-passports), a number of RFID technology experts say this is not true.

[Smart Card Alliance](#) is a not-for-profit association representing more than 185 companies in the banking, financial services, computer and retail markets, including [Gemalto](#), which supplies the RFID inlays that will be used in the US e-passports. The alliance held a news teleconference Tuesday to discuss the demo and address related questions.

In order to ensure interoperability and a base level of security, the nearly 30 countries issuing or planning to issue e-passports have agreed to follow specifications developed by the [International Civil Aviation Organization](#) (ICAO) to establish required and optional types of data that can be encoded to the inlay inside each passport. The ICAO specifications support different levels of protection to reduce the chances of electronic data on one's passport being pulled, or skimmed, surreptitiously, or eavesdropped while the data is being read at a border entry point. A mesh metallic lining on the passport booklets prevents the inlay from being read until the booklet is opened. To protect the info from being pulled by an unauthorized party, the reader's operator must enter a password, written on the passport, to unlock and read the tag, through a process called Basic Access Control. This tool can also be used to encrypt the data on the tag. To access the encrypted tag data, a reader would also need access to the appropriate data keys. Grunwald reportedly pulled all the information he needed to clone his passport tag by reading through the specifications on the ICAO web site.

During the teleconference, Randy Vanderhoof, executive director of the Smart Card Alliance, noted that the data encoded to the chip inside an e-passport is digitally signed and locked by the issuing nation, and could

not be altered even if it was cloned. According to Vanderhoof, what Grunwald accomplished could not serve to make electronic passports less secure because the passport inspectors will still examine the chip's encoded photo and compare it with the person who presents the passport. Cloning a passport's inlay, he says "would be no different, in our point of view, than stealing someone else's passport and trying to present that as your own at a border entry point."

"Electronic passports are far more secure than today's printed documents," says Vanderhoof, because the RFID element is used to authenticate the carrier of the passport through a visual inspection. In the *Wired* story, Frank Moss, deputy assistant secretary of state for passport services at the U.S. State Department, said the e-passport specs were not designed to prevent cloning. "What this person has done is neither unexpected nor really all that remarkable," he told *Wired*, adding that the RFID inlay is meant to be an additional authenticator of the passport's carrier.

What if a country decided to remove the manual inspection process entirely, however, relying instead only on the data presented to an interrogator at a border crossing? In this approach, which the ICAO specifications allow for and which some countries are reportedly considering, someone other than Grunwald could enter a country by presenting a clone of Grunwald's e-passport, as easily as someone could steal an EZPass and drive through a New York toll booth.

"Obviously it would be better to have anticloning features [on e-passports], but [e-passports] may well be more secure than the [ones without RFID], in which photos can be grafted into real passports or inserted into fake ones," says Ari Juels, principal research scientist for RSA Laboratories, the research arm of RSA Security.

Juels says Grunwald's result "is a useful demonstration, but does not really teach anything new. A system with cloneable passports is roughly equivalent in security to a database with integrity protection. Anyone can claim to be another person; the system relies on a physical identity check for its success."

Copyright ©2005 RFID Journal, Inc. All Rights Reserved