

# IBM Proposes Privacy-Protecting Tag

Company researchers claim consumers could reduce a passive tag's read range while retaining its operability.

By Mary Catherine O'Connor

Nov. 7, 2005—Two IBM researchers have created a new approach to addressing privacy concerns surrounding passive RFID tags attached to goods in the consumer supply chain, through what they've dubbed a clipped-tag design.

At this week's Conference of Computer and Communications Security, hosted by the Association for Computer Machine (ACM) in Alexandria, Va., IBM researcher Paul Moskowitz presented a paper describing the tag design and how it could be used. Along with IBM researcher Günter Karjoth, based in IBM's Zurich research lab, Moskowitz coined the clipped-tag concept and coauthored the paper on clipped tags presented at the ACM event.

With the clipped design, consumers would be able to alter the antenna length on a purchased item's tag to reduce its read range significantly. The tag would still be functional, however, and could therefore be used to identify the product for warranty or item-return purposes. Moskowitz says this design would address both consumers' interest in protecting their privacy, and merchants' and manufacturers' interest in keeping the tag usable.

Moskowitz holds 20 patents related to RFID and represents IBM on EPCglobal's hardware action group. He says there are a number of different designs through which the basic principal of the clipped tag could be deployed. In one design, a small strip of printed electrical conductor would link the chip and a short portion of the tag's antenna to the larger part of the antenna. To attenuate the tag's read range, a consumer would scratch off this printed conductor with, say, a penny, just as someone would scratch off the covering of a lottery ticket or prepaid phone card.

Another approach would be to build a perforation line into a tag's substrate, along with a tab that a consumer could pull to remove a portion of the tag's antenna, leaving the chip and a small portion of antenna behind. As a third alternative, part of the tag's antenna could be printed on a removable substrate that a consumer would peel off to reduce the tag's antenna.

With the clipped-tag design, Moskowitz estimates, one could reduce a passive EPC tag's read range from a few meters down to 1 to 2 inches. This would make it extremely difficult to read tags within a person's possessions discretely, because someone with a handheld reader would need to come extremely close to the tags. Should a person attempt to use an amplified, high-power interrogator to read a clipped tag, Moskowitz believes the read range might be boosted to 3 to 6 inches.

To IBM, addressing privacy concerns and discovering ways to protect privacy are very high priorities,

explains Harriet Pearson, IBM's chief privacy officer, which is why IBM supports the development of tools such as the clipped tag. "Technology should enable protection of privacy," Pearson says, who adds that IBM works closely with its partners to study how consumer and/or employee privacy might be compromised through deployments of new technology or business processes.

IBM also has an RFID privacy practice within its business services organization, which offers privacy-related consultation to end users or prospective end users of RFID (see [IBM Announces RFID Privacy Consulting](#)).

Moskowitz says he produced a prototype clipped tag using [Alien's ALL-9338 Squiggle 1.1](#) tag and found that once the tag was clipped, its read range dropped from 2 meters (6.6 feet) to 5 centimeters (2 inches). He admits a clipped tag might require more time or materials to produce and, therefore, might cost more. However, he says, he has not yet discussed that possibility with tag manufacturers.

IBM says it is just now revealing the design to the wider RFID community, and researchers are still very early in the design and prototyping process. Therefore, the company believes it's too early to talk about any business strategy or licensing of the design, for which it has filed a patent.

The EPC Gen 2 Class 1 protocol includes a kill command, designed to address privacy concerns surrounding the threat of an unauthorized party surreptitiously reading tags. The kill command is executed by a reader and renders the tag unusable. The idea behind this command is that consumers could request merchants kill the tags attached to packaging or embedded in products they purchase. This also wipes out the ability of merchants or product manufacturers to use the tag for other purposes. Likewise, it would limit the consumers themselves from using the tag for future applications.

In an [RFID Journal online poll](#) conducted in May, 43 percent of respondents said the kill command is too radical a solution to privacy problems because it limits consumer applications. Another 43 percent said it is not too radical because it is the only way to ensure privacy. Thirteen percent said they were undecided.

Moskowitz notes that while consumers might request a tag be killed, they would have no visual proof any change had been made to the tag, as they would with a clipped tag.

"Also," says Moskowitz, "the kill command is weakly protected with a 32-bit password, which makes tags susceptible to sabotage, especially if all of your tags have the same password. And if you have a different password for all your items, then you, as the administrator of those passwords, need to manage [them all]."

Another idea suggested for addressing privacy concerns is a blocker tag, which can be placed near tagged items to confuse a reader and make it unable to read any item's tag (see [RSA Security Designs RFID Blocker](#)). Moskowitz notes, however, that to use the blocker tags, consumers would need to carry one with them at all times. Moreover, he points out that while tagged items can be placed in metallic bags designed to block tags from being read, some items are too large to store in such a bag.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved