

Can Zero-Knowledge Tags Protect Privacy?

A Danish startup is developing an RFID system that uses a zero-knowledge authentication protocol to protect consumer privacy, while allowing an item's tag to remain alive.

By Farhat Khan

Sept. 27, 2005—A number of techniques have been suggested to protect consumers from unwanted scanning of RFID tags attached to items they may be carrying or wearing. One option is for consumers to carry a blocker tag—a passive RFID tag that can simulate multiple RFID tags and, thus, block an RFID reader from interrogating tags on nearby items. Another method is for retailers to kill item tags permanently when a consumer purchases the products to which they are attached.

Although killing a product's tag at the point of sale may eliminate any potential risk to privacy, it also negates many of the potential benefits of having RFID on items, as well. For example, when tags are embedded in clothing, their EPCs make it possible for an RFID-enabled washing machine to identify the garments and thereby provide the most appropriate wash cycle. And when tagged items are discarded, their EPCs may be used to sort recyclable materials and identify hazardous contents automatically.

A Danish startup named RFIDSec, however, is developing Zeroleak, a new approach to tag security. Zeroleak aims to protect consumers' privacy while allowing a tag to function after the item is purchased. Zeroleak tags will use a zero-knowledge authentication protocol, which can verify that an RFID reader has the proper authority to read it but does not require the tag to reveal any identifying information during the authentication process.

To protect consumer privacy even further, a retailer could put the tag on privacy mode when the consumer purchases a product with an embedded RFID EPC tag. To enable privacy mode, the retailer would delete the EPC from the tag and transmit the tag's EPC and a shared secret device key (SSDK) to a portable RFID reader joined to a PDA or similar device owned by the consumer. In privacy mode, no identifiable information is stored on the tag, but the SSDK would enable the consumer to use zero-knowledge protocol to communicate with the tag and re-encode it with its EPC. That would allow such post-purchase uses of RFID as warranty processing when an item needs repair or recycling when it is discarded.

RFIDSec CEO Henrik Granau says his company is already involved in pilot projects with customers looking for secure RFID solutions. At the present time, however, he is not able to name any of the involved companies. One project is a specialized industry solution involving nonstandard tags but providing a very secure and flexible solution appropriate for this industry. RFIDSec is also working with companies in the pharma industry with a specific aim at providing trustworthy and secure anticounterfeiting solutions, without preventing the additional benefits and business cases of using RFID.

RFIDSec has developed a prototype tag based on the EPC Class 1 Gen 2 standard, but it also plans to offer versions based on other standards. Before the tag is put in privacy mode, it functions as a standard EPC Gen 2 tag and can be read by standard RFID readers. RFIDSec claims its tags will be compatible with EPC standards and services, while offering a higher security level.

The security model upon which RFIDSec is based is a combination of secure RFID tags and managed online security services. The model also includes a patented chip design for secure RFID tags with strong tag authentication, even on passive tags and built-in security. RFIDSec is licensing the technology from Open Business Innovation, a Danish developer of privacy-enhancing technologies. The company expects to mass-produce a commercial version of its tag sometime in 2006.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved