

RFIDsec Unveils Privacy-Protected Tags

The company's RFID system is designed to prevent unauthorized activation of tags attached to consumer products.

By Jonathan Collins

June 21, 2006—Danish RFID startup [RFIDsec](#) announced that its first RFID tags will be available in commercial quantities in the first half of 2007. These tags were designed specifically to protect consumer privacy.

The tag's microchip operates at 13.56 MHz and is based on the ISO 14443-A standard. RFIDsec will be selling tags embedded in RFID labels. The tags work in conjunction with access-management software that permits the encoding and reading of the tag, as well as a product-authentication application to enable owners of tagged products to authenticate the tags. This is designed to ensure that the original tag has not been tampered with, cloned or otherwise compromised.

Based in Copenhagen, RFIDsec also has plans to sell the chips to other tag manufacturers. In addition, the company says that in 2007, it will deliver a UHF EPC Gen 2 version of its chip.

The HF RFID labels will be the first commercially available tags to use the company's RSP (RFIDsec Secure Protocol) security design. The goal of the system is to provide a secure alternative to killing tags at the point of sale (POS). The system is intended for consumers concerned that unauthorized individuals might be able to activate or interrogate any tags attached to the products they buy.

RFIDsec believes that by keeping the tags live but silent its system will allow people to continue using the tags for after-sales assistance or product maintenance, but only when the item owner provides permission to read the tag.

"We are saying, 'Don't kill the tag at the POS—let the tag live, but with ownership transferred to the item owner,'" says Mikkel Winther, executive vice president at RFIDsec.

The RSP systems works by using a 128-bit key to enable access to specific data on the tag, or to authenticate the tag. The key can consist of numerical values and other characters chosen by the item owner after purchase. From then on, unless a reader trying to communicate with the tag knows that key, the tag will not even respond to indicate its presence when in the interrogator's range.

The tag data is encrypted, but the reader communicates with the tag first and the key is never transmitted. As such, says RFIDsec, the tags are safe from eavesdropping.

RFIDsec's access-management software manages the right to read and write data on the tag. According to the company, although its chips are specifically designed to use the RSP system and include additional processing power to manage cryptography, its tags can be read by standard interrogators. However, to switch the tags to and from silent mode, and to encode them, a retailer or other user will need to have RFIDsec software

installed on the interrogator, or on a networked computer that issues RFIDsec software commands to those same readers.

Pricing for the new tags hasn't yet been finalized. "There is no clear picture of cost, as volume [of sales] will play a part, but the only extra cost is on the IC, so it's likely to be a small premium of around 10 percent," says Winther.

According to RFIDsec, the firm has been working on a number of technology trials with other companies, including systems integrators ODIN Technologies and CSC.

RFIDsec aims to allow consumers to manage RFID tags on their goods, but says that won't be truly possible until consumers have their own RFID interrogators capable of switching tags to silent and back again. Until then, Winther explains, the company's RSP designs will be dependant on businesses offering the tag-silencing service to their customers, or be restricted to business-to-business applications.

The company's product plans were announced less than a week after the Danish Consumer Council and the Confederation of Danish Industries issued RFID deployment guidelines suggesting RFID tags should either be killed or transfer their control to the consumer.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved