

Tag Encryption for Libraries

To protect patrons' privacy, a new system encrypts data stored on a book's RFID tag.

By Jonathan Collins

July 14, 2004—Library systems specialists Library Automation Technologies (LAT) has developed an encryption system for RFID communications. Although the encryption system is designed to be used for its RFID-enabled FlashScan self-checkout, which library patrons use to take out tagged books without the assistance of library staff, the company believes it could go on to be used in host of other RFID implementations.

“Libraries have a history of being at the forefront of new technology adoption. They led the way in bar code deployment and the use of large databases. Now, they can lead in RFID encryption,” says Oleg Boyarsky, CEO of Library Automation Technologies, which is based Somerdale, N.J.

The company's new FlashScan RFID Encryption Envelope (FREE) is designed to provide libraries implementing RFID with a way to protect patron privacy. Currently, the only data libraries generally store on an RFID tag is a unique ID number, which is then becomes associated, or linked, to data in the library's back-end system (known as integrated library system, or ILS) so that the library can retrieve information about the book to which the tag is attached. That means that just the unique identification number for a book is transmitted between the tag and the reader.

But an RFID tag could also be used to store other data, including the book's title and author and the name and library card number of the patron borrowing the book. According to ALS, library automation vendors have begun to move toward adding additional data to the tag for purposes of off-line processing.

Libraries use off-line processing as a backup in case their ILS, or back-end database system, goes down, which can be a frequent event at libraries, according to Boyarsky.

“When an ILS goes down, the entire library operation stops,” says Boyarsky. “The only processing that can be done is to write all of the transactions on pieces of paper, which is a very difficult and error-prone process.”

LAT and similar vendors have incorporated off-line processing into their checkout system to allow the library to capture transactions while off line and then later upload into their ILS when it again becomes available. The main difficulty with this, according to Boyarsky, is that if the back-end database is unreachable, it can't be used to validate information on patrons and items or to check policies and user records. Therefore, off-line processing relies on whatever data has been previously loaded into the checkout terminal or on real-time data, such as that written to an RFID tag.

If an RFID transponder is going to store that kind of information, it's important that the tag's data be kept private. As more and more libraries look to RFID to provide an effective way of tracking their collections, civil rights advocates such as the American Civil Liberties Union and the Electronic Frontier Foundation have opposed RFID adoption at libraries that don't implement safeguards to protect the privacy of patrons. The groups want to be sure that if a library encodes tags with any identifiable information, such as a patron's name

and the titles of books he or she is carrying, the library must then ensure that such information cannot be read by unauthorized individuals with an appropriate RFID reader. The American Library Association's Intellectual Freedom Committee is already examining the issue.

LAT's offering requires its FREE software to be loaded on to the Microsoft Window PC controlling a library's RFID network. Working with system that reads and writes to RFID tags, the FREE system generates a "signature" data packet using an internally defined key and algorithm that encrypts the data written to the tag. During that write cycle, the encrypted data along with the signature is written to the tag. The key and algorithm can be changed as often as the Library RFID administrator decides is necessary—even with every book, according to Boyarsky.

When the FREE-encrypted tag is read, its signature is read along with the encrypted data. The signature is then compared with the active signature—the one currently being used by the system—and if they match, then the key on the tag is used to decrypt the data. If the tag's key is not the current key, then the system looks up the key used on the book tag and uses that instead to decrypt.

In order to store the signature, the tags used in library books will likely need more memory capacity than they currently have. The library tags that are widely in use today can hold 1024 bits, or about 128 bytes of data. (Tags that can hold 256 bits, or 32 bytes, of data have been used in the past, but they are being phased out, largely because the cost differential between the two types is negligible.) "Tags need a little more memory to hold the signature but no more than around 12 bytes," says Boyarsky.

LAT's FREE system will be available with all RFID-enabled FlashScan self-checkout systems. The company will also make FREE available for licensing by other RFID library-system software vendors. While the company's key focus for its technology is the library market, it says it can see other markets where its technology could be valuable.

In the retail supply chain, Boyarsky believes encryption will be vital for protecting retailers from potential surveillance by their rivals. Without encryption, he says, entire shipments to a retail store could be read and tracked by any rival that places an RFID reader close enough to goods being shipped. Encryption could also be suitable for high-privacy applications where tags are written to just once and then read many times. One example, says LAT, is using tags to identify blood and other medical samples while ensuring that any patient data stored on the tag is kept confidential.

LAT says its FREE system will be available starting August 10. License pricing, which will include maintenance and updates, will be announced then.

[RFID Journal Home](#)

[Attend RFID Journal University](#)

There are only two weeks left until [RFID Journal University](#) in New York City. This unbiased educational course, presented by *RFID Journal* and members of Auto-ID Labs, is designed to provide the in-depth understanding of RFID and EPC technologies needed to evaluate vendors and begin planning a successful implementation. [Register today](#), or to see complete course outlines, visit [RFID U](#).

Copyright ©2005 RFID Journal, Inc. All Rights Reserved