



Create a more human library

RFID 301

A detailed look at using RFID in your library

For many librarians, the key questions about RFID (radio frequency identification) technology are about ease of use, cost effectiveness and productivity. Others, particularly the library staff members who oversee information technology and systems integration, may want more detail on RFID performance and the differences among tags.

Tag Characteristics

Active tags

An active RFID tag has its own power source (usually a battery). Because active tags can be read from up to 100 feet away, they are very useful for toll road collections and tracking hospital equipment, railcars, and other valuable assets. Because of their bulk and expense, active tags are not used on library or retail items.

Passive tags

Most tags (including those used in libraries and retail establishments) are passive, meaning they contain no internal power source such as a battery. Instead, they are powered by signals generated by readers. Passive tags have several advantages over active tags. First, they are less expensive. Second, they are usually smaller and thinner. Finally, every battery eventually runs down; the absence of a battery significantly extends the useful life of a passive tag.

Passive tag frequencies

Passive tags typically operate at a low, high or ultra-high frequency. This frequency determines a number of performance characteristics, including the distance at which the tag can be read by a reader. The typical read-ranges for commercially available tags are shown below:

Frequency	Low	High	Ultra-high
	128 KHz	13.56 MHz	915 MHz
Range	0-6 inches	0-36 inches	0-15 feet

At present, library systems use high frequency (HF) tags because of their functionality and their read-range. The shorter read-range allows for convenient detection by self-service devices and security gates but doesn't read items on nearby shelves. However, some libraries have expressed interest

in longer-range ultra-high frequency (UHF) tags, which could allow easier shelf management and wider security gate corridors. The advantages associated with UHF tags could also enable certain applications that are not possible with HF tags.

Durability versus cost

RFID tags are typically designed for either supply chain management or asset tracking applications—and the distinction is important. With a supply chain tag (such as those found on retail merchandise), the emphasis is on low cost; durability is much less important because the item will be sold within a few months. In an asset tracking application (as in a library or medical clinic), tag durability is critical. For library tags, materials and assembly processes are designed to ensure that the tag's longevity matches that of the item to which it is attached. In most cases, these tags are slightly more expensive than supply chain tags.

Four Differences Among Tags

Data capacity

Library tags typically have space for 256 bits of information, which is more than adequate for current system demands. Some tags have room for up to 2,048 bits of information. Why spend additional funds on capacity that isn't currently needed? Some library systems want the extra space available in case data requirements change or a new, productivity-improving application is developed.

Read/write characteristics

Most tags have a security code or bit that can be rewritten. When the item has been checked out, the security bit is switched off; when it is checked back into the library, the bit is switched on. With some RFID systems, all other tag information is locked during the original installation. Other systems have unlocked data that can be changed. Why not lock everything except the security code? If the RFID conversion is flawed (due to a dirty barcode, for example) or if a book's unique identifier is changed later, a locked tag must be physically removed and replaced with one containing the correct data. Locked data could also be problematic if emerging standards require changes in data content or formats. Leaving tag information unlocked allows corrections and updates. In theory, it also increases the possibility

of vandalism; in practice, many libraries believe the convenience and functionality of rewritable tags outweighs any risk.

Passwords/encryption

Some library RFID systems incorporate passwords or data encryption features, which are designed to prevent tampering with the data on the RFID tag. This is an effective but unnecessary strategy; to date, there have been no reported cases of tampering with library tag data.

Passwords and encryption are also mentioned as techniques for providing additional privacy for customers; in theory, an encrypted tag would prevent others from detecting which books a library patron was carrying in his or her backpack. Here, too, the strategy is unnecessary. Because of the physics of high frequency RFID tags (such as those used in libraries), readability is limited to about 36 inches. The introduction of next-generation ultra-high frequency tags could extend the read range to an average of around 15 feet; even if this were to occur, an “RFID voyeur” would find only an item identification number, which is identical to the current barcode number and is unique to the library’s database. (This means that the same title would have different numbers at different libraries.)

Passwords and encryption have detrimental effects on inter-library interoperability; libraries that don’t constantly share and update passwords and encryption keys would be unable to read other libraries’ tags. The sharing of passwords and keys would also be expensive and time-consuming, and wide scale distribution would in any case undercut any benefits to security.

RTF versus TTF

All RFID readers put out a constant signal that is available to power up tags that come within range. In a “reader talks first” (RTF) system, the reader also sends out a second “command” signal many times a second. The powered-up tag responds to this second signal with an identifier and pertinent data. Most RFID systems are RTF, and only RTF systems are compliant with ISO 18000-3 Mode 1 standards (see next column). However, alternative (and proprietary) “tag talks first” (TTF) systems are still available. A TTF tag will immediately respond to the reader’s power-up signal. There is little evidence that the difference in response is meaningful for any library functions, including circulation, inventory control or item security.

Evolving Standards

When a technology is first being developed and commercialized, companies apply it in different ways. Over time, industries usually settle on common formats that will allow equipment from different manufacturers to interact. Thanks to these common formats, one manufacturer’s computer (for example) can now operate software from hundreds of suppliers. The

barcode industry has also evolved; even though dozens of manufacturers are now in operation around the world, common formatting allows most modern readers to process a barcode from any of them.

RFID technology is evolving in a similar fashion. At first, individual suppliers created proprietary models. More recently, individual nations (such as Finland, the Netherlands, Denmark and France) have introduced “country-specific” standards; these are designed to ensure interoperability for tags and equipment sold in that country. Leading global manufacturers (including 3M) now offer equipment that has been programmed to operate under these country-specific standards. In locations where such a standard has not been developed (such as the United States), a library can ask one of these global RFID suppliers to program its system in a country-specific standard. Some U.S. libraries, for example, have shown an interest in the French or the Danish model.

These country-specific standards constitute a useful intermediary step in the evolution of RFID formatting, but most participants on national and international standards boards acknowledge that these country standards will eventually be superseded by global standards. For this reason, libraries considering an RFID purchase should pay equal attention to a system’s current standard and its ability to migrate to forthcoming global standards.

The first of these global standards has already been developed by the International Standards Organization (ISO) and other agencies. Many of the “air protocol” standards (which govern how readers broadcast signals and how the tag picks up the signal and responds to it) are in place and are being followed by RFID manufacturers around the world. The most common standard used in library RFID systems is ISO 18000-3 Mode 1; other standards are being developed for other frequencies. Eventually, these air protocol standards will eliminate the threat of “system clash” when a library item tag comes within range of a reader in a retail store, gas station or other location.

Air protocol standards are only a beginning, though. Additional standards, including those that will allow true global interoperability, are under development and should be completed within the next few years.

At a time of emerging standards, libraries need to be cautious about making a major investment in new technology. Three questions are especially critical when considering an RFID system:

- Does the system have sufficient flexibility so that it can be updated when future standards are developed? Experts in the field have a good sense of what will be incorporated in the

forthcoming data format standards, but the specifics won't be finalized for months or years. At a minimum, a library needs confidence that the information that is programmed on its tags today can be rewritten if the new data format standards require a change.

- Will the manufacturer provide a migration path to the new standards? Once a new global standard is approved, each RFID supplier will need to provide a migration path from its current standard (whether it is Danish, French, or a proprietary model) to the new standard. Libraries should expect their supplier to guarantee in writing that it will have available—in a timely manner—the upgraded software that tags and equipment will need in order to comply with a new global standard.
- Will the migration path allow “blended” tag handling? During the transition to the new standards, most libraries will experience a period during which their collections contain both “legacy” RFID tags (that are not compliant) and new tags that reflect the new standards. Libraries must be assured that their RFID system will remain functional during this transition period, which could last for months or years.

Some libraries are understandably reluctant to invest in RFID technology until global data format standards are determined and manufacturers develop systems that are compliant with those standards. This hesitation must be weighed against the immediate benefits to productivity that RFID provides, and against the possibility that standards development could require a lengthy wait. Furthermore—and perhaps more important—manufacturers point out that standards are always evolving. The long-term value of any RFID investment depends on finding a supplier that provides a flexible product and guarantees that its products can be upgraded after an ISO (International Standards Organization) tag-data standard is published.

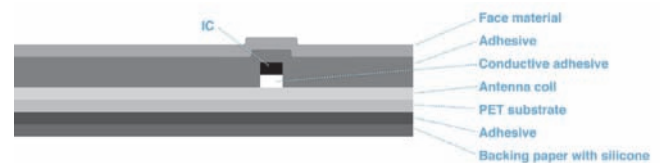
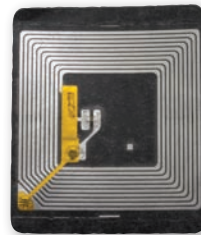
Quality Concerns

The evolution of standards will ensure that RFID tags and readers have common characteristics, but it will not eliminate important quality and ease-of-use differences among systems.

Tag quality is a particular concern. Tag malfunctions are not common but they can occur. (Imagine the stress on a poorly manufactured tag that is adhered to a thin paperback volume, where it is repeatedly flexed and curled. Other stresses occur when a tag is subjected to high temperatures and humidity as it travels from the library to the home and back again.) Unfortunately, poorly manufactured tags are not easily distinguished from more reliable, longer-lasting tags.

When considering the purchase of an RFID system, a library should ask the manufacturer about construction details (including the attachment of the antenna to the microchip, which can be a weak point), the adhesives, and the covering or sheathing, which is a key to protecting the electronics from physical damage and environmental harm (from abrasion, for instance, or humidity).

Leading manufacturers will also provide details on tag testing procedures. Testing should include initial qualification of materials (as well as subsequent supplier audits), but individual component quality is not enough. Each tag is, in fact, a lamination of multiple categories of materials—adhesives, papers, films, chips and metallic antennas—that can have negative interactions with each other. Over time, for example, some adhesives can introduce or accelerate corrosion in the bond between the chip and the antenna.



Exposure to physical and environmental factors can also have deleterious effects on tags, producing corrosion, cracking or other damage. This can lead to total failure — the tag goes “dead”—or a severe reduction in the read-range. Similar problems can arise if fabricators do not understand and control the processes used to combine RFID components. Curing, lamination and the precise registration of RFID components are advanced processes that require sophisticated management and close monitoring to produce a reliable tag. Slight variations in curing time or assembly speed, for example, can have significant impacts on consistency and longevity.

Because most libraries expect their RFID tags to last as long as the items to which they are attached, they are especially concerned about the potential for failure after five or ten years.

The most reliable technique for estimating durability over time is subjecting the tag to “accelerated aging” tests, which usually involve exposure to high heat and humidity. These tests—which are used throughout the electronics industry—last only weeks or months but can reveal flaws that would otherwise become evident

only after a tag has been used for several years in the field. Established RFID manufacturers (those with more than a decade of experience) are now able to compare actual performance with initial projections of tag life using accelerated aging tests, and the results have confirmed the validity of these techniques.

Security Functions

All modern RFID systems incorporate a security function that provides protection against inadvertent removal of materials and outright theft. Three methods have evolved for implementing security features, and the differences among these methods can be meaningful for libraries.

- **Database Look-up** Some systems employ a “database look-up” model, in which the item’s checkout status is logged on a database. When a customer carries an item through a security gate, the gate identifies the item, accesses the database and confirms that the item has been checked out. This approach requires that each item’s full identification number be accessed and relayed to the server for verification. This can be a reliable process when only a couple of items are passing through the gate, but problems can arise when a customer leaves with a larger quantity of books and other items. In some instances, readers do not have enough time to capture the data on all the RFID tags. In other instances, the response time could be too slow for security purposes.
- **Application Family Identifier (AFI)** Under ISO standards, an AFI code is assigned to all RFID tags in a specific application (such as pharmaceutical tracking, baggage handling or libraries). This stops a library book from setting off the security alarm at a shoe store; it also prevents a library book in a suitcase from interfering with a baggage handling system. When a library security system uses AFI, the gate will request a response from any “checked in” library item. When an item is checked out, the AFI code is modified so that the tag does not respond to this request. Because only tags with an unmodified AFI code respond to the security reader, response rates are fast and reliable.
- **Electronic Article Surveillance (EAS)** The EAS approach is similar to AFI in that the status of an item (checked out or not) is encoded on the tag. Also, AFI and EAS systems both require the reader to detect only those items that have not been checked out. The greatest difference is that EAS systems are proprietary (meaning they are not defined by the ISO), which could impact interoperability. In addition, EAS systems do not distinguish between application families. As a result, EAS systems face the unfortunate possibility of not being able to recognize some items within the library (due to interoperability) and yet recognizing—and sounding an alert over—non-library materials (such as a rented video) as they pass through the security gate.

Detuning

RFID tags are tuned to resonate at and respond to a signal at a specific frequency. (High-frequency tags, for example, resonate at the 13.56-megahertz frequency.) When an RFID tag comes in close proximity with metal (such as another tag or a metallic medium like a DVD), it can resonate at a slightly different frequency. This phenomenon is known as detuning. In rare instances, an item might not register because of detuning.

Detuning is much less likely to occur when libraries ask their customers to refrain from checking out of a large stack of CDs or DVDs (checking out fewer items at a time usually eliminates the problem). Many libraries will also stagger the placement of RFID tags, making it less likely that tags on thin items will directly overlap on the checkout pad, or on the shelf during shelf reading or inventory operations.

Viruses and Vandalism

Some libraries have voiced concern over the theoretical threat of RFID virus attacks, which have been described in a number of academic papers. To avoid such an attack, well-designed systems use a carefully defined tag format that is validated for content and expected values. This protects it against malicious exploitation. In addition, a competent supplier will periodically review and update its software to eliminate any potential risks.

RFID vandalism—the destruction of RFID tags in the library or while an item is checked out to a patron—is also a possibility. In its crudest form, RFID vandalism occurs when a tag is defaced or torn off an item. RFID experts have also shown that it is possible to corrupt RFID tag data or to render the tags inoperable using a computer and a commercially available RFID reader-writer. (However, as of this writing, no library RFID system has reported such an attack.)

As with other crimes, the response to RFID vandalism begins with prevention (through the implementation of data protection strategies), vigilance (through normal library security procedures) and full prosecution of offenders when they are caught. At this time, RFID vandalism is a possibility but hardly a probability. Libraries must estimate the threat of RFID vandalism in the context of other risks inherent in any “open door” setting.

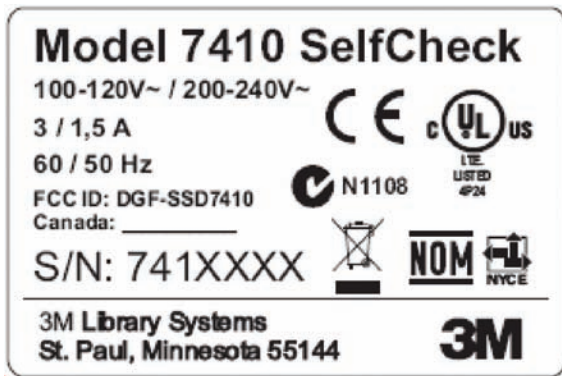
Health, Safety, Accessibility and Environmental Issues

The library is often a centerpiece of a community. As such, it attracts a broad cross-section of the population that includes young children, senior citizens and the disabled.

Given this diverse clientele, libraries must pay particular attention to issues of health, safety and accessibility. Like

other employers, they must also look out for the well-being of their employees. In addition, they are responsible for the environmentally acceptable disposal of equipment and materials.

In many countries, government agencies ensure compliance with health, safety and environmental requirements. In other countries, independent certification organizations perform this function. When compliance has been established, the products are often awarded a seal or mark of approval. The following example shows marks from several organizations and agencies, certifying compliance with requirements in the United States, Canada, China, the European Union and elsewhere.



In the United States and some other countries, the premier certification organization is Underwriters Laboratories (UL), which checks for compliance with product safety regulations. It also confirms that equipment and materials meet the requirements of the Americans with Disabilities Act and workplace regulations outlined by the United States Occupational Safety and Health Administration (OSHA).

Libraries should be aware that OSHA regulations stipulate that equipment be certified by UL or a similar organization. As always, failure to acquire proper certification could have legal consequences for a manufacturer or purchaser if employees or customers are injured by equipment.

Other Performance Considerations

RFID is not an emerging technology. It has been used in industrial and military applications for decades, and its performance and reliability are well documented. In addition, the broadening applications for RFID, especially in file tracking and retail inventory control, have led a gradual reduction in cost that is characteristic of an established technology.

Nevertheless, RFID remains a fast-changing technology. Any attempt to describe performance and tag characteristics will be rapidly outdated. This is especially true with respect to the development of global standards for data formatting.

Libraries will want to ensure that they are purchasing equipment that reflects the latest advances in RFID technology. They should also look for a system with flexibility, so that it can evolve along with new standards as they are promulgated by international standards organizations.

Because upgrades and improvements are inevitable, libraries should be sure to work only with suppliers that have a reasonable track record in the industry, a willingness to guarantee their equipment and tags, and a commitment to continued research and development.