WHITE PAPER

Radio Frequency Identification (RFID)

An introduction for Library Professionals

By Alan Butters

Principal Consultant
Sybis

FIRST PUBLISHED AUGUST 2006

REVISED SEPTEMBER 2010

Table of Contents

Introduction to the revised version

Since August 2006 when the first version of this white paper was added to the Sybis website, it has been downloaded many thousands of times by interested people from all over the world. The white paper is now available for sale on Amazon.com as well as from numerous electronic publishers and has been widely referenced in articles on library RFID. All of this activity is testament to the desire for information on this topic by library professionals internationally.

A revised version of the white paper is long overdue as the application of RFID in libraries continues to evolve. In this updated version I will attempt to provide both new information as well as more current observations on library RFID. Much of the original text will be preserved, albeit with minor editing where required. The major areas that will be addressed in this 2010 version are:

- Standards for RFID in libraries - information regarding ISO 28560 & migration to the new standard
- UHF RFID for libraries - observations on the current status of this technology in libraries
- Functionality - some thoughts on the leveraging of ISO 28560 for enhanced functionality
- Change management - a critical but frequently undervalued part of many RFID projects

It's my sincere hope that this document continues to provide a useful and independent contribution to successful RFID implementations within the library community and your comments or constructive criticism are always welcome.

Alan Butters

September 2010

Executive Summary

At times it seems that Radio Frequency Identification Systems (RFID) are employed in a new application almost every week. Industry analysts predict revenue from RFID sales to grow exponentially over the next decade with the technology seen as an enabler and a major driver of productivity and service improvements. At the same time, many are concerned about the potential loss of privacy that might accompany a move to RFID. Still others are worried about where the standards are heading and whether now is a good time to embrace the technology.

Libraries globally share these kinds of concerns. It can be very challenging for non-specialists to get answers to questions in a form that they can both understand and trust. In many ways the situation with RFID in libraries is reminiscent of a period in the early 1980's when computers began appearing in numbers within libraries. In those days the computer vendor was king. The knowledge gap that existed between the technologists and the library professionals ensured that the market was very much driven by the supply side. Many libraries had no technical experience or capability in-house and were reliant in almost every way on the computer systems vendor. Of course, that has all changed and now libraries are at the forefront in demanding open systems architectures and interoperability etc.

Where library RFID is concerned, the situation hasn't progressed to this advanced stage as yet. While it's common for libraries to have information technology expertise within their organisations, RFID with its seemingly strange blend of radio technology and electronics often appears unfamiliar and unique. It can be difficult for library professionals to evaluate vendor solutions and to weigh features and benefits against standards and frequencies etc. The aim of this paper is to provide some general information and observation which will hopefully put some of the variables into context. Through discussions with libraries over recent years, many areas of concern or confusion regarding RFID have been identified and it's these areas that the paper will principally address. Without going into excessive technical detail, the paper will attempt to cover the important things and to suggest a framework in which to begin further exploration into the world of library RFID.

What is RFID?

Introduction

RFID is a set of technologies that enables tracking and monitoring activities to be carried out using invisible radio waves over distances that range from less than a centimetre to many hundreds of metres. Most often it's employed to track items such as pallets or cartons within a supply chain or warehouse. RFID is also used to identify animals, hospital patients, shipping containers, laundry garments, airline baggage and so on.

In many of these cases, barcodes have been used historically to identify the items concerned. One limitation of barcode technology is that the barcode scanner and the barcode must have a line-of-sight relationship. The barcode scanner must be able to "see" the barcode to operate correctly. This requires items to be presented in a particular orientation to the scanner and every barcode must be visible on the outside of the item. If we imagine a pallet stacked with barcoded cartons, the cartons that are located at the centre of the stack will have their barcodes obscured by the cartons surrounding them. In this case, the cartons would have to be removed for the scanner to read each barcode.

In the RFID world, the barcode is replaced with an RFID "tag" and the barcode scanner is swapped for an RFID reader. The tags are essentially smart labels in most cases and have a microchip and antenna as their main components. In our pallet stacked with cartons example, a suitably placed antenna would be able to read the RFID tags on every carton in the stack almost instantly and without requiring them to be visible. The radio waves generated during the reading process are able to penetrate many materials and so can be employed where tags are not visible to the eye.

RFID in Libraries

RFID's property of non line-of-sight operation can be very useful within a library. If we replace the barcode traditionally used to identify library material with an RFID tag containing the same item number, we are immediately able to process multiple items simultaneously and the tag can be located inside the cover in the case of printed material. No longer does every item require individual handling. The benefits can be realised in improvements to productivity, service, materials handling and collection management etc.

RFID tags for libraries come in a range of sizes, commonly measuring approximately 50mm x 50mm and having a paper backing on one side and an adhesive layer on the other side. Several suppliers are also now offering larger tags having dimensions similar to business cards or credit cards and which provide modest performance improvements in some contexts. Special RFID tags are available from some vendors for CDs, DVDs and video cassettes. There are even tags available with "repositionable" adhesive allowing them to be reused again and again on material such as periodicals etc. Tags for traditional library materials can usually be over-printed with the name and logo of the owning institution if required. The RFID tag may be used not only as a barcode replacement but may also contain additional information such as the library and branch identifier, material type and even the title if required. In many cases the RFID tag is also used for item security and so takes the place of the electromagnetic security strip as well.

RFID in the world outside libraries

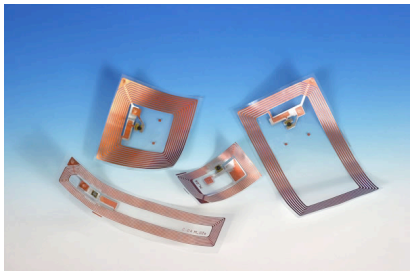
The history of RFID

Many histories of RFID trace the roots of the technology back to a seminal paper in 1948 by Harry Stockman entitled "Communications by means of Reflected Power" (Shepard, 2005). Much pioneering work was done in the late 1930s and early 1940s which resulted in the technology we now know as radar. While it was obviously useful to be able to detect an object at distance using a primitive radar system, it was even more useful to be able to determine the identity of the object. This requirement (given added impetus by World War II) led to the development of Identification - Friend or Foe (IFF) systems. These two technologies, radar and IFF, conceptually form the beginnings of what we know today as RFID.

The point for library professionals is that the idea or principles of RFID have been around for quite some time. The application of the modern technological expression of these ideas is obviously more recent, particularly in the library community.

RFID systems today

One of the most confusing things about RFID is that it is not one single technology. This fact is often the cause of misconceptions and misinformation carried by the popular press, a topic we'll return to later. The reality is that the way RFID readers communicate with RFID tags varies from application to application, as does the frequency at which they communicate. The good news is that within the library world, almost all systems operate at the same frequency and and use the same or very similar technical principles.



Passive tags

Semi-passive tag

Active tag

Different types of RFID systems in use today

Broadly, RFID systems employed across current applications differ in three ways:

- The way the electronics on the RFID tag is powered
- The method of communication between the tag and the RFID reader
- The frequency at which the two communicate

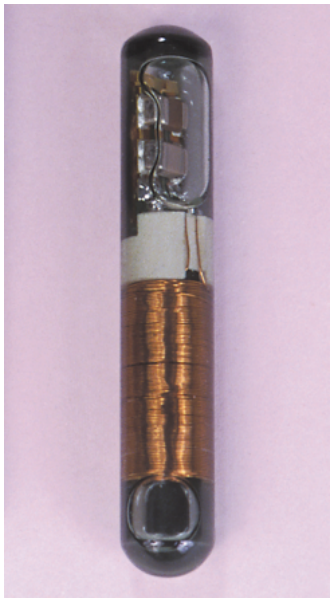
Why do these differences exist? Because differences along these three dimensions provide a range of performance characteristics that enable RFID systems to be employed across a broad spectrum of applications - each with its own requirements. It's probably worth spending a short time providing some examples. As the pictures above illustrate, RFID tags come in many different shapes and sizes. The pictures show examples of three types of tags; Passive, Semi-passive, and Active. The most meaningful thing to be said about the differences between these tags is the way that they are powered. The Passive tags have no battery to power them (Lahiri 2006) and so they draw their power from the elec-

tromagnetic field generated by the RFID reader - quite a neat trick. It will be obvious from the pictures that, for the library application at least, a tag without a bulky battery will be essential if the tag is to be placed inside a book.

The other two tag variants shown in the pictures both have batteries (Glover and Bhatt, 2006). The Semi-passive tag uses its battery to power its internal chip whenever it is interrogated by an RFID reader. These sort of tags are used in vehicle tolling systems such as the Citylink system in Melbourne Australia (Transurban, 2001). The Active tag uses a larger battery to transmit its signal over a greater distance and so permit monitoring of objects hundreds of metres away. So the first thing we can say is that the physical size of the tag may be important in some applications (such as libraries) whereas the read-distance may be more important in others.

We also said that RFID tags differ in the frequency range in which they operate. This concept shouldn't be too foreign to us as we're all familiar with devices that operate at different frequencies. We know for example that if we wish to listen to a particular radio station we need to tune our receiver to a specific frequency. In this way the radio stations are kept separate and don't interfere with each other. Similarly, while we might not worry too much about whether FM radio waves are affecting our health, we are more concerned about using a mobile phone on a regular basis. Most of us are also very familiar with the heating effect that microwaves produce in anything containing moisture. The point here is that these devices operate at different frequencies and at these frequencies the electromagnetic energy produced has different characteristics or behaviors (Finkenzellar 2004). This fact is used to good effect by RFID manufacturers who split operating frequencies into several ranges such as low frequency, high frequency, ultra-high frequency, microwave frequencies etc. Frequency range is chosen to suit the requirements of each application. Two examples will illustrate this:

Animal Tagging



Here is a tag that's routinely injected under the skin or into the muscle of companion animals such as cats and dogs (and sometimes they're even injected into humans). What would be the set of performance requirements for an RFID system used in this application? Firstly, the tag must be small and we can't realistically remove it to swap batteries so it must derive its power over the air from the reader. So, a Passive tag is needed. Secondly, the nature of the application means that we will always have to read this tag through a layer of tissue - skin, fat, muscle etc. Because of this fact, we need to choose our frequency carefully. Why? Remember that we said different frequencies have different characteristics. Within the RFID world, one of the important differences between frequencies is how each one performs in the presence of water.

As a general rule we can say that the higher the frequency, the less penetration the electromagnetic field achieves through water. In fact we depend on this characteristic to heat our food in a microwave oven which operates at a much higher frequency than many of the other devices with which we are familiar such as radios and mobile phones. If the microwaves simply passed through our food, the heating effect would be minimal. Because the microwave energy is absorbed by the moisture within our food, the food is heated. In our animal example, the various layers of animal tissue that we need to penetrate in order to read our tiny RFID tag are made up mostly of water. So if the field from our RFID reader is absorbed by the water component of our animal's tissue instead of passing cleanly through, it might make our animal warm (or worse) but there certainly won't be enough power left by the time the field reaches the tag to power up the chip for normal operation. Therefore, in this application we need to select a low frequency system which permits the RFID field to easily penetrate through to the tag. Because the operator has the animal in one hand and the reader in the other, we also don't need extended read-range and so a low frequency passive-tag system fits the bill.

The point to keep in mind as we proceed is that the useful characteristics of our low frequency system are unique to this system, not generic qualities of all RFID systems. This point will be significant when we discuss issues of privacy later.

Vehicle Tolling Systems

For our next example we've chosen the application of vehicle tolling systems. These systems employ an RFID tag within each vehicle, usually mounted somewhere near or attached to the front wind-screen. The data on the tag is linked to an account on a remote computer and each time the vehicle passes a fixed point, the tag is read and the attached account is debited for the trip. The picture shows a system in Singapore but such systems are in use worldwide. What might be the requirements for an RFID solution for this application?

Obviously, the factors we considered in our animal tagging application are not the ones important here. Probably our first concern would be how quickly we might need to read the tag for our system to work correctly. After all, the vehicles are usually traveling at speed - often freeway speeds. The next problem is that we must read the tag successfully from quite a distance - the overhead gantry on which our RFID readers are mounted has to be high enough to allow the passage of large trucks etc. Also at this reading distance, it will be almost impossible to power the tag from the reader - the reader's power diminishes very quickly with distance. So, read-range, read-speed, and tag power will be our three most serious concerns.

Fortunately we have enough space inside each vehicle to allow a bigger tag than could be injected into our companion animal so we can choose a battery powered tag. A feasible scheme can also be designed to replace the batteries when they are exhausted. We'll choose either a semi-passive tag or an active tag, both of which have batteries. Which to choose? Semi-passive tags are used in the systems within Australia (Transurban 2001). These sort of tags signal to the reader by reflecting some of the reader's power back (similar to a radar system) but use their internal battery to power the chip when it's needed. These tags usually operate at frequencies in the microwave range. This suits our application due to another variable along the frequency dimension; the higher the frequency, the greater the data transmission speed that can be achieved. Our semi-passive tag gives us the read-speed, the read-range, and the internal power we need.

For the sake of completeness, when we would we choose an Active tag? As a general rule, these are required when even greater read ranges are required - perhaps hundreds of metres. Having larger batteries, they are able to power not only their internal chip but also to boost the transmission power and achieve distances far beyond their semi-passive cousins.

Once again, the point to remember for our later discussions about library RFID is that the characteristics of our RFID tolling system are entirely different from our animal tagging system. No single RFID technology platform possesses all of the things we need in all applications. There is no one-size-fits-all in RFID.

RFID in the library application

Introduction

RFID systems have been in existence within libraries for more than a decade. Various vendors claim to have installed the first RFID library system but we can say that somewhere in the mid 1990's, commercial RFID appeared in a library somewhere in the world. During the following decade, usage accelerated but penetration remains relatively low. Over the last few years, RFID tag prices have continued to fall steadily to the point now where, in most system quotes, the total cost of the tags no longer represents the biggest single line item on the page.

A question often asked about RFID is: "Should we buy now or should we wait for things to get cheaper/better/more standardised?" etc. There is obviously no universal answer to this question but, once again, the situation reminds us of the first decade of library computer systems. At that time (indeed, as now) everyone knew that systems would improve over time. They would, and did, become cheaper, faster, smaller, more functional, and more standardised. So why didn't libraries wait to buy? Some did but many didn't. The real question for those libraries in the 1980's was this; does the purchase of a library computer system give my library demonstrable service/productivity/management benefits right now? If the answer was yes, regardless of where in the constant path of evolution these library systems existed, many libraries signed the purchase order and reaped the benefits. Of course they knew that things would change and in a few years their system would be upgraded. The point was that the system gave their organisation real benefits in the meantime.

> The decision regarding whether to buy into RFID now or to buy later should be determined by an assessment of the real benefits to the organisation at any point in time...

My view is that RFID is in the same situation. Will the tags get cheaper? Yes. Are standards becoming clearer over time? Yes. Will we end up with much improved interoperability between systems? Probably. All of these things could reasonably be expected to happen as the future unfolds. The important questions are these:

- Do we really know what we want RFID to deliver in our library or can we devise a process to find out?
- Are there systems on the market that can deliver what we want?
- Can we construct a positive & realistic business case to demonstrate that the benefits justify the cost?
- Do we have the skills and experience (or access to them) to make the right system evaluation/selection?

If the answers to these questions are all positive, it makes sense to proceed in a structured way. Many libraries have done the analysis and proceeded to implement RFID. Most appear to have achieved their expectations, a few have been disappointed and later we'll look at some of the reasons why.

Technology

Following our previous discussion about various RFID technologies and frequencies, we could perform a similar analysis on the library application of RFID. Of course, this decision has largely already been made for us but it might be useful to briefly explore the reasoning that was used.

Obviously the first challenge in selecting a library RFID system is the size and the cost of the tag. We essentially need a smart-label application that can be attached to library material in a relatively unobtrusive way - a passive tag of some sort without a battery. The tag needs to be flexible and durable. We need to read the tag over a distance of at least half a metre. We need the field to penetrate the tissue of borrowers with books under their arms (as well as the moisture contained within the pages of the books) if we use the RFID tag for security. We'd also like to be able to read a stack of tags (in a stack of books) very quickly so that we can improve productivity for our staff and the self-serve experience of our borrowers.

The best compromise fit with all of these factors was deemed at the outset to be high-frequency passive tags operating at 13.56 MHz. This frequency offered a good balance between data transfer rate and moisture immunity. The additional good news regarding this frequency was that it was available for use with RFID in just about every country in the world (Paret 2005). Library vendors adopted it and it has become the dominant tag / frequency combination used in libraries around the world today.

More recently, there has been interest shown in using Ultra High Frequency (UHF) tags which operate at close to mobile phone frequencies (920 MHz in Australia) within the library application. These tags are traditionally found in supply chain management and logistics applications. In the next section we'll return to this topic to consider UHF tags for libraries in more detail.

Useful things to know about library RFID

Privacy & Data Security

The comment was made previously that because RFID is based on multiple technology platforms and frequencies, confusion often exists regarding what can and can't be done with the technology by a malicious adversary (Mather and Wiebell, 2005). This confusion is seen particularly in the area of privacy and concern appears strongest in the United States where privacy issues for libraries are hotly debated (O'Connor 2005; EFF, 2005; Ayre, 2005). Hopefully by now, when analysing what an adversary might or might not be able to accomplish, we can see that such a person or agency would be limited to some extent by the restrictions of the RFID technology chosen for a particular application. Unfortunately, this fact is often overlooked in the debate. Sometimes it's assumed that because an RFID tagged shipping container might be trackable at a distance of 100 metres, a person's library books might be scanned by someone hovering over their house in a helicopter. I have heard this very example used in discussion about the risks of library RFID.

RFID is not one single technology platform about which generalisations may be made. Particularly in the area of privacy, caution is needed to limit comments to application areas...

Let's put aside for a moment the issue of who these helicopter-equipped adversaries might be or what their interest in our reading habits is that prompts them to go to such lengths. The question to be asked is whether this or a similar scenario is possible. In the case of our high frequency library RFID systems, and for reasons that we have already touched on, the answer is no. We observed that our library application employs passive tags. An explanation of exactly how a passive tag derives its power from the RFID reader and communicates is beyond the scope of this paper but, suffice it to say, the physics involved in the process set an upper limit on the distance over which communications may take place. An important point to note is that this maximum distance exists *regardless* of the power of the reader. For tags operating at 13.56 MHz (as in the majority of libraries) this distance is approximately 3.5 metres. So, no adversary will read RFID-tagged library material from a helicopter, or from the roof of a building across the street, or from any position outside a distance of 3.5 metres. In reality, even achieving a 3.5 metre range would be a serious challenge.

We can say, therefore, that many of the extreme scenarios that sometimes arise are simply rendered impossible by the physics involved with the type of RFID technology employed by libraries. An analogy (if somewhat lighthearted) could centre on a being from another planet performing a review of the transport systems on the earth. A superficial report to our alien's superior might indicate that, on earth, motor cars are wonderful devices - they can carry seven passengers, they can travel at 300 kilometres per hour, can climb steep hills and forge rivers, can haul large boats and travel 1000 kilometres on sixty litres of fuel. The reality is that *each* of these things is true in the case of individual cars but no one car possesses *all* of these attributes. The car chosen to haul large boats is unlikely to travel 1000 kilometres on sixty litres of fuel, for example. So it is with RFID. One cannot generalise about possibilities across multiple applications as the technology used in each application may well be different.

So if the extreme examples are unrealistic, what is possible for a well equipped adversary? Certainly a covert RFID reader could be installed in a doorway, or as part of an airport screening system. Possibly a covert reader could be carried by an adversary and, should he or she get sufficiently close, could read the tags on library books carried by another. Most (but not all) of these sorts of privacy attacks assume that the adversary has access to additional information not carried by the RFID library tag. This is particularly true where the tag has only the item number - the number that is or was represented by the barcode. To derive the title from the barcode requires access to the library's computer system. If the adversary has the titles and tag-numbers correlated then this adversary could possibly use that information to screen passengers with specific materials as they attempt to board an aircraft, for example. From a technical perspective this would be entirely possible.

Many other forms of potential attacks have been described such as tracking, profiling and hotlisting (Molnar and Wagner, 2004; Albrecht, 2006; Givens, 2006). A detailed analysis of all of these falls outside of the scope of this paper, as does the increased theoretical potential for digital vandalism when employing RFID within the library (Tanenbaum et al, 2006). Libraries having specific concerns or who want more detailed information should seek expert assistance.

Many libraries take a pragmatic approach to the issue of borrower privacy with RFID. There are many lists available containing tips for implementation contexts where privacy is an issue; here is my list:

- Don't use RFID tags for borrower cards – if an RFID borrower card is required, employ specific, purpose-built proximity card or smart-card technology, not a laminated RFID book tag.
- Reduce the amount of data on each RFID tag – putting only the primary item ID on the tag may assist in the customer-relations effort where privacy is expected to be an issue.
- On the library OPACs, don't allow item searches by the public using the barcode – this reduces the likelihood that the item identifier and the title can be easily linked.
- Ensure that transparency exists with regard to library RFID projects – this serves to help manage expectations and fears within the population of library users. High profile cases of covert RFID testing have been exposed in the retail area and have generated much negative publicity for the organisations involved.
- Review security procedures generally – as some of the attacks mentioned depend on matching external information to the data on the RFID tag, ensure that the library is secure in all its practices and policies, particularly in the area of information and communications technologies. Consider a specialist audit.
- Lobby vendors for improved security solutions – while not of immediate benefit, much development work could be done to improve the security status of RFID systems based on current standards. These include:
    - Development of anonymous ID systems using randomly generated numbers on issued tags paired with real accession numbers on the library database.
    - Improved authentication of readers.
    - Improved password protection.
    - Solutions based on ISO / IEC 18000-3 Mode 2 or other standards etc
- Support research into library specific solutions for current RFID privacy concerns.

Standards

Libraries have been aware of the benefits of standardisation and open systems for many years now and so it is not unusual to be asked about the situation with regard to RFID standards for libraries. The bad news is that there is no library-specific standard for RFID tags and hardware in existence. However, most RFID vendors have "commandeered" a smart-card standard from outside of the library application area and used part of this standard in the library smart-label application. While this standard doesn't meet the needs of libraries in all areas (data security and therefore privacy is one), nevertheless it's a start. When a library RFID vendor claims their solution to be "ISO compatible" what the vendor is saying is that it employ tags conforming to ISO 15693 parts two and three or ISO 18000-3 Mode 1 which is the latest incarnation of this standard (to be precise, the former is a perfect subset of the latter). These standards define things like command sets for communication, modulation, timing etc.

What does this really mean for libraries? It means that the same physical tag may be used in systems from two vendors that both support the standards mentioned. Unfortunately it does not mean that the two systems will have interoperability. The reason for this is not obvious at first glance.

When an ISO compatible library RFID system uses an ISO compatible RFID tag, it first formats the tag to accept library data. This is analogous to the use of a hard drive or a USB drive in a PC. A truly blank (unformatted) drive cannot be read or written to by the computer - it must be formatted magnetically before data may be written to it so that the PC knows where the data resides on the drive and how it may be retrieved. The same situation exists with a blank RFID tag. The problem is that the standards previously mentioned don't specify *how* the data will be formatted - that is how it will be arranged in the tag's memory. So RFID vendors have been required to devise a formatting scheme of their own. They have all done this and in most cases their schemes are unique and often proprietary. When an ISO tag from vendor A is read by vendor B's system, the second system cannot interpret the data contained on the tag as it knows nothing about its format. It doesn't know for example, where individual data fields start and stop, how the data is encoded, and even how many data objects the tag contains. So despite both system's ISO compatibility, there exits no interoperability between the two libraries involved *once their tags have been formatted by their respective systems*.

Clearly this is not what libraries expect from standardisation and several national initiatives arose during the last decade in an attempt to overcome this difficulty. Some, such as the Danish, Finnish, and Dutch groups have finished their work and have developed de facto standards for their own countries (RFID, 2005; FIND, 2005; NBLC, 2004). More recently, ISO, the international standards body, has been developing a new standard aimed at international interoperability. This standard, known as ISO 28560 is about to be published in final draft form and will be available for purchase from www.iso.org A detailed discussion of the new standard is beyond the scope of this white paper but some general information may be provided in the form of an overview.

ISO 28560 has three parts. The first part is a list of data objects or elements that libraries might choose to place on their RFID tags. These elements relate to bibliographic or item specific data - examples include the title, the MARC or ONIX media format, the owning institution identifier etc. This list may grow over time but in the final draft standard there are about thirty elements. Part two of the standard takes these data elements and encodes them on the RFID tag in an ISO standardised way and allows freedom by individual libraries in the selection of which elements they will employ. Only one data element is mandatory for all RFID tags under part two - the primary item identifier (most likely the barcode number). The standard also contains a "content parameter" element - analogous to a table of contents for use in situations where several data elements are present on the tag. Using a combination of parts one and two of the standard, libraries have complete control over which (if any) data elements they will employ in addition to the mandatory primary identifier.

Part three of the standard takes the same list of data elements from part one but takes a different approach to how these will be used on the tag. Instead of giving complete flexibility to the library in terms of data element selection, part three organises the data elements into sets known as Blocks. Instead of a mandatory *element* (such as the primary item ID in part two) part three employs a mandatory *set of data elements* called the Basic Block. The Basic Block includes the primary item ID but also includes the owner library code, set information, and a type-of-usage parameter. In addition to the Basic Block, part three of the standard allows for Extension Blocks containing other sets of elements aimed at acquisitions processes, inter library loans, enhanced item identification etc.

Astute readers will have already perceived that in fact ISO 28560 represents two standard ways of encoding the data on a library RFID tag, not one. That this is the case is somewhat unfortunate as is the fact that part two encodings and part three encodings are not necessarily interoperable at the tag level. This outcome (as opposed to the ideal of a single international method of organising tag data) came about because of deeply held differences of perspective within the ISO group responsible for the standard and a perceived need for backwards compatibility with the widely used Danish Data Model. Considering these differences, an entirely possible alternative outcome might have been that no international standard was developed at all. Given this context, having essentially two encoding options in the standard was

deemed preferable to having no standard. It is hoped that the selection of part one and two encoding or part one and three encoding will be made on a national basis, in this way at least providing interoperability within individual countries. In addition, ISO 28560 employs a specific mechanism to assist RFID system developers to determine whether a tag their system is presented with conforms to part two or part three. While it's early days yet, it would appear that at least some countries have made their preferences clear regarding encoding. It seems that Australia, New Zealand, the USA and the UK will favour the flexible part two encoding scheme while at least Denmark will employ part three encoding for their libraries. Obviously there is a real need in each country adopting ISO 28560 for education within libraries so that national interoperability is not compromised.

Given that many libraries already have RFID implemented while others are planning for the technology, what might libraries do in preparation for the new standard? The following are offered as suggestions:

Ensure that no new RFID implementations employ locked tag data. This will be required so that the RFID tags within existing library material can be reconfigured to the new data model standard. Locked data on tags cannot be unlocked.

Ensure that a prospective RFID vendor commits to the new standard. It's suggested that a commitment to implement ISO 28560 within an agreed timeframe (such as twelve months) be included in tender and contract documentation.

Ensure that you get the data on to the tag that you want to use under the new standard. If a seamless migration is to be made from an existing data model to the new standard, any dynamic data elements that might be required by the library under ISO 28560 will need to be present on the tag already. In this way, the data held on the tag in an old format may be read and then written back in the new standardised format as part of a circulation process such as returns. If a call is needed to retrieve external data to add to the tag during this process it is likely to be considerably slower.

Choose vendors that have a demonstrable track record in supporting open systems and standards. The new ISO standard could well offer opportunities for enhancing functionality of the RFID system as a whole. Vendors who demonstrate support for open systems might be more willing to explore such possibilities than those who do not.

Organise a working group to explore ways to educate library communities. It has been my observation that some libraries have no real understanding regarding tag data models or even which data elements their RFID vendor is currently encoding on their RFID tags. Library professional bodies could facilitate much useful educational work in preparation for the introduction of the new standard. Issues of data profiles and minimum interoperability data sets should be widely considered now and will be further discussed in a later section.

Obtain a statement from your RFID supplier about the transition plan. For libraries with existing RFID systems there exists an issue of migration to the new standard. Some vendors are already promising seamless conversion to the new data model, perhaps at the point of material return.

Leveraging ISO 28560 for interoperability and enhanced functionality

As stated previously, the main thrust behind the new standard is to enable a common data format and therefore a level of interoperability between different vendor's RFID solutions. For most libraries this means having the ability to read RFID tagged items from other libraries who may be part of a consortium or other cooperative arrangement. In this context, what is being delivered by ISO 28560 is to restore what libraries already had when using barcodes for identification. While this is obviously a step forward from the current situation, it isn't the only benefit deliverable by the new standard and the following sections provide additional possibilities for consideration.

Selection of data elements

A barcode attached to an item represents one data element - the item identifier. To gain additional bibliographic or item level information requires the use of the item identifier as part of a database lookup. This system has served libraries

well for many years and also makes considerable sense as the majority of the information pertaining to the item is stored in one place - the database of the library management system. Many individuals see no reason why this model should not be preserved under RFID and therefore the item identifier is often simply copied to the RFID tag's memory and the tag functions as a sort of smart barcode. One of the differences with RFID under ISO 28560 is that for the first time libraries will have choice - in the case of systems built on parts one & two of the standard, the choice of the specific data elements to be used. This means that when moving to the new standard, individual libraries will need to make a decision regarding what sort of information they wish to place on their RFID tags. Why would a library consider putting data elements on the RFID tag beyond the unique identifier? There are probably many reasons but consider these examples using specific data elements available under ISO 28560:

- Data element - MARC media format

This data element represents a MARC 21 category of media descriptor and is a compound of two letters defined by position 6 and 7 in the leader of a MARC 21 record. There are many uses for this element, for example:

Many RFID implementations now employ lockable circulating cases to allow CDs and DVDs to be securely borrowed by means of self service. The unlocking mechanism is incorporated into the self service system ensuring that these items do not leave the library without sounding the alarm if they have not been borrowed and unlocked. Unfortunately, many libraries are not consistently able to identify these items due to variable cataloguing practices. Placing the media format on the tag itself removes any database variability and also allows the self service systems to operate correctly in the event that the library management system is unavailable due to system or network failure.

- Data element - Type of usage

The type of usage data element provides additional qualifying information about the item, for example the type of material and its use within the library. Examples include:

The identification of non circulating material in situations where the self service systems have no access to the library database due to a server or network outage. Employing this element on the tag allows the self service unit to prohibit the loan of reference material for example when the library management system is unavailable. Other examples include the identification of library equipment for loan, the discrimination of borrowers and material where RFID is used for membership cards and the indication of special handling required for certain items when using sorting systems such as fragile, over or under sized items etc.

- Data element - Set information

Set information consists of two components: "number of parts in item" followed by "ordinal part number". These two component parameters are used to identify various permutations relating to material sets. There are numerous uses for this element including:

The identification at the staffed returns point that all items in a set are present without the need to check – DVDs inside locked boxes or book / disk combinations etc. With automated returns systems, the prevention of an item return when part of the set is missing – the case returned but the DVD left behind in the borrower's player for example. Also the detection of a missing set component at the time of loan through a self service loans kiosk etc.

Context based data

The fact that RFID tags are rewritable opens up the possibility of having different combinations of data elements based on the current usage context. For example, in the acquisitions phase it may be possible to populate the tag with information relating to the item, the supplier and the specific delivery. A library receiving such an item may then scan the RFID tag and have the information that is retrieved from the tag automatically populate fields within a procurement application or even within the library's software management system.

Once the acquisitions information has been retrieved, the normal circulating profile could be automatically written to the tag in preparation for shelving. It may even be possible to use ISO 28560 data elements to construct a self managing interlibrary loans system based solely on tag data - the possibilities to leverage value from the standard are many.

The point is of course that the RFID tags may be written to thousands of times and each usage context may call for a different combination of data elements. New and useful possibilities exist where ILMS suppliers and RFID suppliers work together to use the standard to add value in ways that were simply not possible before.

Item Security

Many libraries choose to abandon their electromagnetic (EM) security systems in favour of using the RFID tag for both identification and security. The advantages are obvious in requiring the application of only one tag and the savings associated with security strips and processing costs. When it comes to security, there are several options on the market which may be broadly summarised as:

RFID tag based security is not as strong as traditional EM security. However, item security options must be weighed by each library along with other features and benefits...

1. Two tag systems - one RFID tag and one EM tag in each item
2. One tag systems using part of the RFID tag's memory to indicate the security status of the item
3. One tag systems that employ server-based security and don't rely on part of the tag memory for security
4. One tag systems that employ proprietary technology on the tag to perform the security function

Which of these systems is to be preferred? What advantages or disadvantages are associated with each option? Obviously a detailed analysis lies outside the scope of this paper but some broadly-based (and necessarily subjective) observations may be made regarding the various options.

Let us start by addressing the first two options which essentially represent a choice between EM security and RFID security. Firstly, there is no solution that suits all libraries - no single superior choice for everyone. Much depends on where item security sits in a library's hierarchy of requirements. The fact that in existence are libraries with no security, libraries who have EM gates installed but not actually switched on, and libraries who employ two sets of security gates back to back, suggests that not all libraries feel the same way about security. It is true, however, that libraries in general (with the possible exception of many in the school library sector) have historically chosen EM security over RF based security. There are many reasons for this including the ability to circulate tagged material easily etc., but a key driver is the superior detection rate of EM when compared to the simpler and cheaper RF systems often found in retail stores. EM systems are harder to defeat and the security tags are usually covert and hard to spot or remove. Now, RFID and RF security are not the same thing but RFID tags used for security do share some of the failings of traditional RF security tags.

Most noticeable is their sensitivity to orientation within the detection area, and their vulnerability to being masked. There are certain orientations, or angles of presentation within the detection area of the gates, which make it more difficult for the passive tag to be powered by the reader's field. In these specific orientations the tag might not be read at all and so the security status of the tag (or even the actual presence of a tag) cannot be determined. Also, two tags in close proximity to each other (overlapping wholly or partly) can prevent either tag from being read. For this reason, some vendors offer dual EM security / RFID identification configurations as part of their solutions.

So is RFID tag-based security to be avoided? Not necessarily - it depends on the requirements. A question that's often asked is; "How much worse or less-effective is RFID-based security than EM security?" Obviously a definitive answer is not possible as it depends (among other things) on which vendor's systems we are comparing. Experience suggests that an average RFID-based security solution will have about 80% to 85% of the detection performance of an average

EM solution in real world use. Obviously that's a conclusion based on observation and not on empirical data. Some vendors may do better, others might be worse. That number may be good enough for many libraries. I have often been told over the years that simply having a set of security gates on display solves 80% of the problem anyway. If you have sympathy with that view you're unlikely be troubled by the shortcomings of RFID tag-based security. If not, you will need to evaluate each vendor's solution more critically in this area.

It should also be noted that the above comments apply specifically to the standard security systems available from many vendors. Increasingly, what are known as 3D security gates are appearing in RFID solutions - sometimes at a cost premium over their standard 2D predecessors. The promise of the 3D gates is superior detection which is said to close the performance gap between EM security and RFID based security - in all orientations. Prospective purchasers would be well advised to carefully evaluate the cost/benefit of all options prior to purchase.

What about options three and four on the list? The third option is an interesting one. In this scenario the tag is not used for security in the traditional sense but a cache of recent transactions is held on a server attached to the local network and when the tag's identity is read, its eligibility to leave the building is checked against the cache of transactions. Thus eligibility to leave is determined directly as a result of an actual checkout transaction. The most common implementation of this option came from Checkpoint. When this server-based system is combined with a WORM tag which is contact programmed, some significant security benefits are generated including immunity from many over-the-air digital vandalism and security-bit Denial of Service scenarios. Of course, this is achieved at the cost of increased Information Technology complexity and requires additional hardware.

The fourth option are systems where additional technology is added to what otherwise might be a standard tag to provide an Electronic Article Surveillance (EAS) function - sometimes described as tag-talks-first solutions. Vendors claim that such systems offer increased performance when compared to systems using a part of the tag's memory for the security status. Personal observation would suggest that this claim has some merit. I would suggest that, if the detection performance is particularly important, tests be carried out on systems under consideration using both single items and multiple items in the detection field with items presented in several orientations. An hour spent in this fashion should provide some comparative results which can then be weighed in the context of other factors for or against each system such as the need for specific RFID tag types to enable the security function etc. Each library will need to establish their own weighting for item security within their overall set of requirements. Libraries who want to gain more detailed information regarding item security should seek expert help.

High Frequency or Ultra High Frequency for RFID in libraries?

Readers who require a more detailed discussion of this topic than is appropriate in this paper are directed to the white paper *"RFID for Libraries - A comparison of High Frequency (HF) and Ultra High Frequency (UHF) options"* available from the resources section of the Sybis website - www.sybis.com.au What follows is a summary of the significant issues.

As mentioned earlier, one of the attractive features of developing library RFID systems that operate in the High Frequency (HF) range was that the allocation of spectrum at 13.56 Megahertz is available in most countries throughout the world, being reserved for industrial, scientific and medical applications. Use of this frequency ensures that a supplier's RFID system will be saleable in almost all countries and for this and other reasons most suppliers selected HF. However, RFID technology continues to evolve and today there exists other technology options that might also be used as the basis for a library RFID system. One of these options that has received attention is Ultra High Frequency (UHF) RFID as commonly seen in the supply chains of major organisations such as Wal-Mart and the US Department of Defense. These systems do not operate at 13.56 Megahertz but instead use frequencies between 860 and 960 Megahertz determined by local regulations within each country. Again, for the purpose of context, this frequency range is more commonly encountered with mobile (cell) phone communications. Some suppliers of RFID tags and components take the position that if library RFID systems were being developed for the first time today instead of fifteen years ago, UHF

would be the logical technology platform. HF systems as used in most library systems worldwide are therefore seen by some to be legacy systems belonging to a bygone era and not as part of the future of library RFID.

In Australia there are several libraries using RFID systems based on UHF and several others exist in countries around the world. The white paper mentioned earlier provides greater detail but the following is offered without comment as a summary of the commonly perceived pros and cons of UHF technology versus HF technology within the library application.

The case for UHF in libraries

- UHF tags and readers are cheaper to purchase than HF equivalents due to the volumes used in other applications
- UHF tags may be read over significantly greater distances than HF tags
- Data may be read from UHF tags at significantly higher rates than HF tags
- UHF tags are less easily masked by proximity to each other than are HF tags
- UHF tags represent the future of RFID

The case against UHF in libraries

- There is fundamentally no interoperability with the majority of libraries still using HF RFID
- There are perceived health risks associated with electromagnetic fields at UHF frequencies
- UHF systems are relatively new and not all products as are as capable as their HF counterparts
- Most UHF tags have very little user memory
- UHF electromagnetic fields are more difficult to control than HF fields in the library context
- UHF has been placed out of scope in the new ISO 28560 data model standard

UHF RFID technology holds promise for libraries. It seems however that UHF library vendors are not making the progress that they would like in the library market. A fundamental lack of interoperability with existing HF systems is a concern for many libraries as are hard-to-shift perceptions about UHF fields and OH&S.

What to make of all this? When all is said and done, the benefits that RFID can deliver to libraries are real. There are suppliers in the market today with proven track records in successful implementations around the world. The reality is however that RFID technologies are still evolving and are driven by markets and industries that dwarf libraries in terms of their potential size. There exists no one having an RFID crystal ball and able to predict with certainty how the RFID landscape will look five or ten years from now. Possible future outcomes include scenarios where neither HF or UHF dominate the competitive landscape. In the meantime, libraries have businesses to run and customers to satisfy in the contexts of changing user expectations and often uncertain budgets. So should libraries hold off on purchasing any RFID system until this gets sorted out? Remember the debate over VHF or Beta video tapes? Both of them were leapfrogged by DVDs. In the future, DVDs themselves will be made redundant, perhaps through some sort of online delivery. This never ending process of evolution didn't stop millions of consumers enjoying the benefits conferred by videotapes, even though millions more have since replaced such systems with hard drive recorders and DVDs.

As with home entertainment systems, so with RFID. The important questions for library professionals are these; Does this system, regardless of whether it is based on HF or UHF platforms, allow us to achieve the goals and targets we have for *our* library service? Does it support *our* strategic vision and meet operational requirements - including interoperability requirements? Is it well designed and constructed for reliability and ease of use by staff and borrowers?

Does it do all this to the extent that we can construct a positive business case to secure the needed funds? If the answer to these questions is yes, an acknowledgment that the technology might (will) be different in ten years from now should not stop us from proceeding and realising the benefits. As with most technologies, if we wait it will likely be cheaper, smaller, faster, more standardised etc. But in the meantime, there are libraries to run and genuine benefits to be realised.

RFID Solutions for libraries

From the foregoing it will have started to become obvious that there are many differences between RFID library vendor's solutions on the market. These differences are seen, for example, along the following dimensions:

- Solution focus
- Systems architecture
- Functionality of individual components
- Product range
- Product maturity
- Size, market penetration, representation
- Price
- Vendor capabilities & experience
- Attitude toward & compliance with standards

How to choose a system? This can be a challenging task and the next section discusses an approach that I recommend and which many libraries have found to contribute towards a positive project outcome.

How to begin an RFID investigation

How not to begin

My experience in speaking with libraries about technology over the past twenty five years or so has been that in many cases, when information is required regarding a new technology, the first person to be called will likely be from a company already used as a technology supplier to the library. However, this is not always the best way to begin. In this commercial world it would be unrealistic to expect totally impartial advice from a party who stands to benefit from your purchase. However, in my view, that libraries turn to a trusted technology supplier is not the real problem. It could even be argued that at least these suppliers have a vested interest in maintaining a long term relationship with their customers and so would be unlikely to sell them a wholly unsuitable system.

RFID library vendors can be very helpful to libraries during a project but the library should first define what a picture of project success looks like within its own operation...

I think the real problem lies with *at what stage* libraries choose to approach the market. While it can be easy to pick up the phone and make a call, when an environment exists where there is great variability in the solutions offered, as is the case with RFID library systems, it is always risky to attempt to evaluate advice without really knowing what's important in one's own case. It's only when a very clear picture of local requirements, expectations and targets exists that a meaningful evaluation of features and benefits can be made.

A better way

It can be a non-trivial exercise to establish what specifically is required in order for an RFID implementation to be declared a success. I have known of libraries that have entered into projects with no real vision of the outcome other than generalities concerning productivity and service. Let me provide an example to illustrate. If we were to compile a list of the promised benefits to our library through an implementation of RFID, it would probably look something like this:

- Increased productivity outcomes
- Improved Customer Service
- Streamlining of materials handling - improvements to OH&S
- Improved collection management
- Enabler for future functionality
- Optimising Self Serve loans & Self Serve returns

While lists may vary from person to person, almost all would include these things. If we took such a list to all the libraries in our area and asked the library management team whether these things were important we would almost universally receive the same answer - yes. However, if we tried to insist that all of these benefits were of *equal* value then we would probably be met with an argument. A benefit that is key to one library may be of little relative importance to another. For example, collection management might be the single benefit most sought by one library whereas another might be focussed almost exclusively on productivity gains. In my experience, even when two libraries rank productivity gains as their primary target, even then the organisations might actually want two different outcomes.

So, we have an environment where there are significant differences in the strengths and weaknesses of vendor's RFID solutions and we have requirements that are not prioritized in the same way across all libraries. This would suggest that it is possible to choose systems that could be both suitable or unsuitable for our specific requirements. This is not to say that a given system might bring no benefit to an organisation. Rather, what's required to gain maximum benefit is that the strengths within the system chosen must match the critical factors for success within the library. This means that the library must have a very clear vision of what those success factors are *before* approaching the market. To do

otherwise is to risk having the success factors influenced by the pitch of a specific vendor. This is a particular risk when the knowledge gap between the systems supplier and the library is great.

My suggestion is to hold a workshop with key people to evaluate exactly what the priorities are for a successful migration to RFID. What does the word "productivity" mean to this organisation? How would we describe a successful implementation of the technology? What would it mean for the staff? For the borrowers? What would change and what would remain the same? Can we be very specific about what we expect to gain?

These are important questions that deserve our time to explore. The answers can sometimes be challenging, controversial, and surprising. Once armed with a clear picture of success however, a library is in a good position to weigh the benefits offered by current systems. The prioritized and weighted requirements statement becomes the lens through which all suppliers and their solutions are evaluated. Libraries that don't have access to the necessary experience and skills to reach this position should seek outside assistance at this crucial stage.

How to get more information

There are as yet not very many good published sources of unbiased and independent information specifically for libraries, however publications that do exist include:

- *Radio Frequency Identification Handbook for Librarians. Connie K. Haley, Lynne A. Jacobsen, Shai Robkin. Published by Libraries Unlimited.* A good general introduction, if somewhat USA focussed.
- *Making the Most of RFID in Libraries. Martin Palmer. Published by Facet Publishing.* A good general introduction from a librarian in the UK with some excellent information on managing an RFID implementation within a public library service.

Of course, more and more libraries are embracing RFID and their experience should be considered as a minimum. The websites of the library RFID vendors are also a good place to begin to gather information for a comparative study. There are also consultants specialising in RFID within libraries (including the author) but not many as yet. Most books on RFID, if they mention the library at all, do so only in passing. The author's website has a number of links which can be followed for more information on standards, privacy, vendors, and general RFID matters. For those interested in the technical detail, the book *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* by Klaus Finkenzellar (Wiley) is probably the best general work. *RFID and Contactless Smart Card Applications* by Dominique Paret also has some good technical information about systems based on ISO / IEC 15693.

For a discussion of RFID privacy issues, the book *RFID, Applications, Security, and Privacy* edited by Garfinkel and Rosenberg (Addison Wesley) has a number of interesting chapters including one on privacy within libraries. The paper by Molner and Wagner listed in the references gives an overview of the technical challenges involved in creating a secure platform using current RFID standards.

Conclusion

I have attempted to touch on a number of areas within this paper while trying not to get bogged down in detail or technical jargon. Clearly, more attention may need to be given to specific areas before committing to a system. Libraries are well advised to consult broadly and to invest time developing critical success factors before commencing discussions with vendors. As with many projects, the time invested at the start is often reflected in the quality of the outcome.

About the author

Alan Butters is Principal Consultant at Sybis, a Melbourne based technology consultancy focussed on the needs of Australian libraries. Alan specialises in Library RFID systems and process-automation technologies such as self-serve loans & returns and materials sorting. Alan has more than twenty five years experience within the library sector including roles managing product development laboratories tasked with generating innovative solutions for the global library market.

Alan chaired a working group within Standards Australia that developed a standards proposal for an RFID-tag data model for Australian libraries. He is a member of the ISO TC46/SC4/WG11 RFID standards for libraries working group and a member of the ACS, IEEE, and ALIA, and has served on the committee of VALA.

Alan has a Masters Degree in Digital Communications from Monash University.

Brief Glossary

- **Active Tag**

Generally used term for an RFID tag that contains a battery powering both the tag's transmission as well as the onboard chip.

- **Air Interface**

The wireless free space through which the RFID reader communicates with the RFID tag via a specific communication protocol

- **Antenna**

A conductive device designed to receive or radiate electromagnetic energy. In RFID systems, antennas may be used to both receive and transmit data modulated electromagnetic energy.

- **Chip**

The silicon component containing the memory and processing capacity of the RFID tag. The chip is very small when compared with the attached antenna. Memory capacity varies between chip types.

- **Electromagnetic Spectrum**

The range of electromagnetic radiation characterised in terms of frequency or wavelength.

- **Frequency**

The number of cycles a periodic signal (such as a radio wave) executes within a given time. Usually expressed in Hertz (cycles per second). RFID systems operate at thousands of Hertz (kilohertz), millions of Hertz (megahertz) or billions of Hertz (gigahertz).

- **Inductive Coupling**

The process by which power is transferred from the RFID reader to the tag using a magnetic field without contact. Method of powering passive tags.

- **Interoperability**

The ability to use tags, components and modules from different RFID vendors within a single system.

- **Memory**

A method of storing data in an electronic form. Within RFID tags, memory capacity is expressed in Bits.

- **Open Systems**

In the world of RFID, the ability to capture, store, handle and communicate data according to defined standards and between systems.

- **Passive Tag**

An RFID tag without a battery that is powered by inductively coupling to the reader. Power is transferred by the electromagnetic field of the reader.

- **Programmability**

The ability to enter and to change data stored in an RFID tag's memory.

- **Protocol**

A defined set of rules governing how (for example) an RFID reader communicates with an RFID tag.

- **Read Range**

The maximum distance between the RFID reader and the tag at which the tag may be effectively read. This distance is affected by the power output of the reader, the orientation of the tag in the field, the method of communication, and the electrical environment.

- **Read Rate**

The maximum rate that data can be communicated between the RFID reader and the tag. Expressed in bits per second.

- **Tag**

Generally used term for an RFID transponder.

- **Transponder**

An electronic device that can both Transmit and Respond - an RFID tag.

- **WORM Tag**

Write Once - Read Many. A tag that is programmed once and then can subsequently only be read.

References

Albrecht, K. (2006) *RFID: The Doomsday Scenario.* RFID Applications, Security and Privacy, Addison Wesley, 259-273

Ayre, L.B. (2005) *Wireless tracking in the library: Benefits, Threats, and Responsibilities,* RFID Applications, Security and Privacy, Addison Wesley, 229-243

Electronic Frontier Foundation (2005) *Keep RFID's out of Californian Public Libraries!* Retrieved from http://www.eff.org/Privacy/Surveillance/RFID/

Finkenzeller, K., (2004) *RFID Handbook - Fundamentals and applications in contactless smart cards and identification.* Wiley 11-28

Finnish Libraries RFID Working Group, 2005 *Finnish Data Model* Retrieved from http://www.lib.helsinki.fi/katve/toiminta/docs/RFID-DataModel-FI-20051124.pdf

Givens, B (2006) *Activists: Communication with consumers, speaking truth to policy makers*. RFID Applications, Security and Privacy, Addison Wesley, 432

Glover, B., and Bhatt. H. 2006 *RFID Essentials* O'Reilly 58

Lahari, S., (2006) *RFID Sourcebook*, IBM Press. 9-10

Mather, K. and Wiebell, H. (2005) *RFID should be restricted by the state*. Information Age December 2005 / January 2006 - Australian Computer Society

Molnar, D. and Wagner, D., (2004) *Privacy and security in library RFID - Issues, practices and architectures* CCS'04 October 25-29 2004 Washington DC, USA

NBLC Netherlands Association of Public Libraries (2004) *Generic Set of Requirements RFID for public libraries, Version 03-00* Retrieved from http://www.dbc.dk/medier/intspec02-10.pdf

O'Connor, MC., (2005) *San Francisco Library denied funds for RFID*. RFID Journal. Retrieved from http://www.rfidjournal.com/article/articleview/1708/1/1/

Paret, D., (2005) *RFID and contactless smart card applications.* Wiley, 91-93

RFID Data Model for Libraries Working Group (2005) *RFID Data Model for Libraries - Proposal for a Data Model*. Retrieved from http://www.bibliotheca-rfid.com/docs/dokumente/Datenmodell.pdf

Shepard, S. (2005) *Radio Frequency Identification* Mc Graw Hill, 42

Tanenbaum, A. and Crispo, B. and Rieback, M. (2006) *Is Your Cat Infected with a Computer Virus?* Retrieved from http://www.rfidvirus.org/papers/percom.06.pdf

Transurban (2001) *Electronic Toll Collection Roadside Systems - Familiarisation Course* Transurban, Edition 1