Designing public libraries for RFID: trends and opportunities

Alan Butters *Principal Consultant, Sybis.*

Radio Frequency Identification (RFID) systems designed for libraries continue to evolve with a focus on enhancing the customer experience and delivering improved productivity outcomes for library staff. As libraries across Australia and New Zealand embrace the technology as a part of their baseline ICT infrastructure, the number of application areas for RFID technology outside of libraries is also expanding. With RFID becoming a fundamental tool across a range of sectors, increased attention is being paid to issues of interoperability, OH&S, privacy & security and integration with existing systems, processes and spaces. In many ways, libraries are at the forefront in addressing some of these issues and have the opportunity to demonstrate best practice in the future.

RFID systems have been operating in Australian libraries for more than a decade now. During that time, a transition has occurred from proprietary to standardised RFID hardware followed by a transition from proprietary to standardised systems of storing library information on RFID tags. The number of suppliers in the market has increased and the flexibility, complexity and capability of library RFID systems has grown. The requirements and limitations of RFID are now routinely factored into the design and layout of library buildings as well as the structure of library fittings and furniture.

This paper looks at four issues that are impacting or potentially will impact upon library RFID systems and some of which will need to be considered when designing spaces that include RFID affected workflows.

Near Field Communication (NFC) Equipped Smartphones

NFC capability is to be found in most modern Smartphones such as those manufactured by Samsung, HTC, LG, Motorola, Nokia, Sony etc. Just one Samsung model, the Galaxy S III has sold over 50 million units since its introduction in 2012.[1] The technology is probably most easily understood by considering it as a type of RFID, not too far removed from the RFID systems that are now common in libraries. This NFC capability allows Smartphone devices to be used in new ways and applications. One of the more significant possibilities for NFC equipped Smartphones is for the device to act as a credit card using the card emulation mode of NFC. A world is thus envisaged where the Smartphone replaces a range of cards including credit and debit cards, loyalty cards, transport cards etc.

While NFC has been present in mobile phones for almost a decade, recent developments should cause libraries to reassess the threats and opportunities arising from the Smartphones carried by their members. What has changed the status quo is the decision taken by the world's largest manufacturer of NFC Smartphone controller chips to support ISO 15693, the standard most commonly employed in library RFID systems[2]. The upshot of this decision is that most new Smartphones, combined with an appropriate app, are able to read and write to library RFID tags.

While this new capability opens the door to a range of new application possibilities including self-service loans using Smartphones and library RFID tags, it also enables a number of negative and possibly malicious interactions. The reality is that in almost all libraries throughout Australia and New Zealand there will be a number of users possessing the basic hardware to erase, alter or lock the information stored in RFID tags by using apps that are freely available over the Internet. A number of potential attacks on library RFID infrastructure are possible including denial of service attacks and theft of library material by disabling the RFID tag-based security.

Of course an adversary has always been able to purchase RFID hardware with a view to engaging in digital vandalism in the library. However such an attack would be relatively isolated and limited in scope. With 268 million NFC equipped Smartphones expected to ship in 2013[3] and able to act as RFID reader / writers, the development of a library-specific app designed to damage RFID infrastructure could have a wide ranging effect and this within a very short period of time. So the threat to library RFID systems from digital vandalism has changed over the last two or three years.

While a complete discussion of this topic and the mitigation strategies available to libraries is beyond the scope of this paper, an overview may be provided. The actual options open to a specific library will be determined by a number of factors including what type of RFID chip is installed in the library's RFID tags, the capabilities of the RFID system hardware and the manner in which the data is stored on the RFID tags. Perhaps one of the simplest methods that might be used to partially mitigate the threat from Smartphone enabled digital vandalism is to lock the library information stored in the memory of the RFID tag.

If a library has migrated to ISO 28560, the new data storage standard, this library might choose to lock some or all of the data on their RFID tags. Locked data cannot be unlocked but it also cannot be changed by a Smartphone-wielding adversary. ISO 28560 permits selective locking of data elements and so provides some powerful capabilities in terms of protecting tag data. Of course a library which has not yet migrated to the new standard should be cautious about adopting a locking strategy as this would prevent a move to ISO 28560. However, it would be quite feasible to adopt a locking strategy as part of the migration process to the new standard, thus accomplishing two goals simultaneously.

For ISO 28560 equipped libraries, an absolute minimum approach might be to lock the item's unique identifier (the number previously encoded by the barcode) for all new items added to the database. This would protect the item's identifier, which, even though other tag based information might be lost in an attack, would allow the library to continue circulating the item.

More comprehensive strategies are also available which involve the potential to password protect the AFI value (the RFID tag's system memory field used by ISO 28560 as an item security status indicator), or a migration to alternative security methodologies including the Electronic Article Surveillance (EAS) function employed in chips from NXP Semiconductors. Of course these options should be evaluated according to the perceived level of risk for each library service and with an awareness of any implications that such options might carry.

It would likely be wise for libraries having concerns in this area to commence discussions with their RFID suppliers to ensure that options are available for new items entering the collection as well as escalation strategies should the threat level increase in the short to medium term.

ARPANSA RPS-3 Compliance

Electromagnetic Radiation (EMR) is radiated energy that is produced from natural sources such as the sun as well as from most electrical and electronic equipment such as computers, photocopiers, televisions and radio transmitters etc[4]. Issues of health and safety in relation to electromagnetic radiation have existed in libraries for many years and most particularly in relation to item security systems. Indeed, health and safety concerns led many libraries to switch off their electromagnetic (EM) security systems in years gone by and many remain inactive to this day.

The rise of RFID systems in libraries has resulted in a new focus on EMR as of course central to the operation of such systems is the generation of radio frequency fields. It is not uncommon (or unreasonable) for library staff to question the safety of a new RFID system with which both they and the library's users are required to interact. While the question of health and safety is a simple one to ask, the answer has been considerably more difficult to provide. Recent testing at St Kilda library, the main branch of the Port Philip Library Service (PPLS) in Victoria, has allowed a more authoritative answer to be given and may be of interest to many other libraries.

PPLS employs an RFID system supplied by FE Technologies and the components of this system were the subject of an EMR evaluation project that spanned eighteen months and which concluded in November 2012. The testing was facilitated by the author of this paper and was carried out by EMC Technologies, one of Australia's leading testing and certification organisations.

For the purposes of the EMR testing at PPLS, the type of radiation involved is known as non-ionising, radiofrequency radiation. As a generalisation, non-ionising radiofrequency radiation, unlike ionising radiation from X-rays and radioactive materials, lacks the energy to essentially break chemical bonds and to damage living tissue[5]. Non-ionising radiofrequency radiation is generated both naturally from the sun and the ionosphere as well as from a great range of electrical devices.

The applicable standard is known as ARPANSA RPS-3. ARPANSA is an acronym for the Australian Radiation Protection and Nuclear Safety Agency. ARPANSA is a Federal Government agency, part of the Health and Ageing Portfolio and is charged with responsibility for protecting the health and safety of people and the environment, from the harmful effects of ionising and non-ionising radiation. The standard *Radiation Protection Standard - Maximum Exposure Levels to Radiofrequency Fields - 3 kHz to 300 GHz.* Was released by ARPANSA in 2002. This radiofrequency standard sets limits for human exposure to non-ionising radiation within a broad frequency range into which, toward the lower end of the range, the RFID equipment at PPLS falls.

Six components of the RFID library solution supplied by FE Technologies were evaluated during the project period to identify their EMR emissions against the ARPANSA standard. The testing occurred in three phases that included initial baseline testing before installation, testing at FE Technologies premises once EMR mitigation strategies had been developed and then finally after the equipment had been installed at St Kilda library. The components tested were:

1. The Smart Bin
2. The small circulation staff pad
3. The item security gates
4. The standard circulation staff pad (without a power attenuator)
5. The standard circulation staff pad fitted with a power attenuator
6. The self-service kiosk

The testing done by EMC Technologies was both complex and thorough. The standard allows for two sets of exposure limits – one for occupational exposure and another for public exposure. Occupational exposure is workplace exposure where staff are trained in EMR safety etc and public exposure limits relate to members of the public who may not even be aware that EMR fields exist at a particular location. Needless to say, the public exposure limits are stricter. At PPLS, EMC Technologies determined that all of the testing should be accomplished using the public limits as the library staff could not really be categorised as “occupational workers” under the spirit of the standard.

Following the initial baseline testing, FE Technologies embarked on an EMR mitigation program to ensure that the company’s equipment operated in the most EMR efficient manner. Consideration was given to issues such as:

- The minimum field strength required by the RFID components for correct functionality.
- The management of RF fields so that these were only active when they needed to be.
- The duty cycle for each component, reflecting real world usage.
- Any required exclusion zones around products where individuals could not be located for prolonged periods.
- Explicit installation documentation to allow controlled exposure for staff and library users.

Following this program and subsequent testing, the RFID system was deemed to comply with the ARPANSA standard when installed and operated according to the manufacturer’s guidelines. This onsite and independent ARPANSA compliance testing is possibly the first of its kind in ANZ libraries and provides a definitive answer to the question of OH&S compliance where EMR fields are concerned.

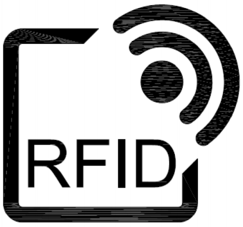
Of interest in the context of the *By Design* conference is the qualification that ARPANSA compliance depends on equipment being installed according to the supplier’s written instructions. This has potentially two implications. Firstly that some existing installations may not comply with the newer installation requirements and secondly, that new installations including those in new buildings will need to comply in order to meet the ARPANSA requirements. The planning and layout of new or renovated libraries may need to take into account some restrictions arising from the results of this testing project. While the installation requirements are not likely to be onerous for new buildings, these must be considered nevertheless.

Of course libraries that already have RFID systems from suppliers other than FE Technologies and who share concerns regarding EMR will need to discuss the compliance of their individual systems with their particular supplier.

Emerging RFID Privacy legislation in Europe

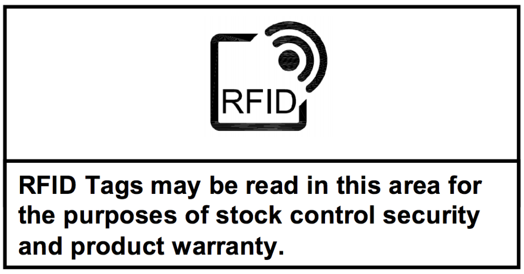
The issues of privacy and data security are of concern to many people around the world. Libraries planning to implement RFID are sometimes asked to address these concerns due to real or perceived threats arising from the covert reading capabilities of the RFID technology. While there is a great deal of misinformation and hyperbole regarding library RFID and its potential to expose an individual's private information, the topic itself obviously remains a valid one.

The European Union, comprising twenty-seven individual countries with a wide range of privacy laws, has made considerable progress around the development of some common legislation to deal with privacy and data security issues relating to RFID implementations[6]. After commencing work in 2006, the European Commission released its recommendations and shortly after these were mandated for implementation by the CEN, CENELC and ETSI standards bodies. Completion of this work is expected in 2014. One of the aims in this project is to provide a level of confidence in the minds of the public that the security and privacy of their information is being respected when RFID is implemented within an industry sector. Particular sectors have been identified and one of these is the library sector. While there are multiple aspects to the project's deliverables, two of these can be mentioned here; signage and Privacy Impact Assessments (PIA).



The signage aspect involves what is called an "emblem" or graphic that must be displayed wherever an RFID system is employed. This emblem will be standardised and therefore common to all RFID implementations in all industry sectors and will alert the public to the fact that an RFID system is in operation. All RFID equipped libraries within the European Union will be required to display this emblem.

The second aspect concerns the development of PIAs, which formally document the potential impacts on privacy resulting from the RFID implementation. These must be developed according to standards and in conjunction with other documentation outlining the capabilities of RFID systems in the privacy and data security contexts and will include interactions involving NFC equipped Smartphones.



RFID Tags may be read in this area for the purposes of stock control security and product warranty.

Of course the European legislation does not directly apply to libraries in Australia and New Zealand but many concerns regarding privacy and data security are shared by all libraries and by library users worldwide. Once these new initiatives become mandatory for European libraries, it is likely that other countries will be prompted to examine their own situations and perhaps to implement appropriate requirements. These developments should be watched with interest.

Returns automation

Increasingly libraries are turning to item returns in an attempt to extract staff productivity benefits from their RFID implementations. There are now a number of returns automation products available that employ RFID in various ways to produce more efficient processes. These products include:

- RFID self returns kiosks

- Smart chute products
- Smart bin products
- Tunnel reader products for items in crates
- RFID equipped materials transport and sorting systems

Perhaps more than any other RFID components, these products can have a significant impact on the design of the library and the workflow and traffic flow within it. These products can also be the most difficult to retrofit into an existing library and so their impact should be well understood when contemplating a new or renovated library building.

Some of the factors to be considered when designing a building or library layout incorporating returns automation products include:

Building security

Quick and convenient after-hours returns of library material is becoming increasingly important for many libraries. However, this provision can potentially open the building to a range of dangers from malicious activities. Uncontrolled access to the library building by means of after-hours returns chutes has resulted in a number of cases where significant damage has been caused by flooding, fire or otherwise unwanted materials or objects. A growing range of products exists to control access to after-hours return and potentially to log or otherwise record return transactions. There are also several options for fire control and suppression including fire rated returns bins, active fire suppression systems using carbon dioxide etc.

Other factors also play a part such as lighting levels, visibility and sight lines, security cameras etc. Determined by the local risk analysis, such systems can have a significant impact on the design and layout of library buildings and their immediate surroundings.

Materials transport

While many libraries focus on the sorting of returned materials to achieve process efficiencies, the transport of returned materials can in some cases be even more important. This is particularly true where the library operates over multiple levels. While there are systems available that will allow returned library material to be transported both vertically and horizontally, it is almost essential that the specification of such systems is done in tandem with design of the building and associated spaces. To achieve a penetration through the library floor after the building is completed, for the purpose of transporting returned material may in practical terms be simply impossible.

OH&S

The implementation of returns automation technology has the potential to reduce the manual handling by staff of library material. However, it also has the potential to introduce new processes and workflows and therefore to create manual handling tasks that did not previously exist. Care must be taken when designing spaces and workflows to ensure that the technology employed does not solve one set of problems at the expense of creating another.

Traffic and workflows

An increasing interest exists in the self-return of library materials. This takes many forms and may involve the users of the library interacting with RFID equipped kiosks or other devices. This process often occurs in a location adjacent to the self-service loans activities and planning is needed to ensure that the two do not negatively impact on each other or upon other users entering or leaving the building.

Staff workflows are also impacted by returns automation technology and thought is needed when considering the use of space and the selection and location of furniture. The ability to return items in bulk using RFID presents a number of challenges that must be addressed if maximum efficiency is to be realised.

Maintenance

Automated materials handling and sorting systems have reduced in price during the last few years and are being routinely investigated by libraries wishing to improve the efficiency of returns handling. Such systems require a relatively high level of maintenance and in the planning for buildings employing such equipment, appropriate access for service personnel must be provisioned.

Learning outcomes

- NFC equipped Smartphones and European privacy legislation may have an impact on library RFID systems within ANZ libraries in the near future.
- Compliance with ARPANSA requirements should be factored in to the layout of new or renovated libraries.
- Increased focus on returns-automation technologies will have an impact on library design and layout.

Notes and references

1. Petrovan, B., 2013, Galaxy S3 sold 50 million units, demand for Galaxy S4 deemed “explosive”, *Android Authority, retrieved 12 October 2013, from http://www.androidauthority.com/galaxy-s4-demand-galaxy-s3-sales-197892/*

2. Balaban, D., 2013, NFC Smartphone chip shipments in 2012 surge past projections*, NFC Times, retrieved 12 October 2013, from http://nfctimes.com/news/nfc-smartphone-chip-shipments-2012-surge-past-projections*

3. IHS, 2013, NFC-Enabled Handsets to Grow Nearly Tenfold from 2012 to 2017, *retrieved 8 November 2013 from http://www.isuppli.com/Mobile-and-Wireless-Communications/MarketWatch/pages/NFC-Enabled-Handsets-to-Grow-Nearly-Tenfold-from-2012-to-2017.aspx*

4. ARPANSA, 2012, Understanding Radiation, *retrieved 8 November 2013 from http://www.arpansa.gov.au/radiationprotection/Basics/understand.cfm*

5. ARPANSA, 2012, Radiation Basics – Ionising and Non Ionising Radiation, *retrieved 8 November 2013 from http://www.arpansa.gov.au/radiationprotection/Basics/ion_nonion.cfm*

6. CEN, 2009, Radio Frequency Identification, *retrieved 8 November 2013 from http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/RFID.aspx*