RFID for Libraries

Standards Australia Working Group IT-019-01-02

Proposal for a Library RFID Data Model

Standards Australia WG IT-019-01-02
Contact: Alan Butters (Chair)
Sybis
PO Box 52
Nunawading, Victoria 3131
Australia
Phone: +613 9878 6447
Fax: +613 9877 0749
Email: alan@sybis.com.au

Status: Draft 06 September 2006

Table of contents

Table of contents 2
Purpose of this document 3
Introduction 4
Background 4
Working Group 4
Standards 5
ISO/IEC 18000-3 Mode 1 5
ISO/IEC 15961 & ISO/IEC 15962 5
ISO 15511 5
Approach to the Data Model 6
Architecture 6
Basic approach 6
Privacy 7
Performance 7
Tag memory usage 8
Long term objectives 8
Scope 8
Conclusions 8
Stage one 9
Stage two 9
Data Model Proposal 10
Overview 10
Data Elements 11
Data Element 11
Description 12
Primary item ID 12
Owner institution 12
Type of usage 12
Usage Qualifier 13
Set Information 14
Media Format 14
Item title 17
Secondary item ID 17
Supplier ID 17
Invoice Number 17
Order Number 18
Security 18
Privacy 19
Implementation 21
Stage one: 21
Stage two: 21
Examples of data model options 22
Next Steps 23
References 24

Purpose of this document

The purpose of this document is to describe a Radio Frequency Identification (RFID) tag data model and standards approach appropriate for the needs of Australian libraries. It is anticipated that the model and approach will have wider applicability. The approach taken is to allow the maximum flexibility possible to individual libraries while not sacrificing interoperability. Acknowledgment is given to the fact that any proposal, if successful, will need to be implemented by library RFID vendors and so must be not only suitable for use by libraries but also commercially viable to implement. This approach recognises also that the library sector encompasses several distinct library types including Academic, Public, Corporate, Special and School etc. and while a common subset of requirements may exist in all cases, individual sectors may have specific requirements.

The proposal acknowledges the work performed by other groups and individuals around the world including:

- NBLC Netherlands Associations of Public Libraries
- RFID for Libraries Working Group (Danish Standard S24/u4)
- Paul Chartier – Praxis Consultants (Bsi Doc IDT/2/7.0003/06)
- Finnish Libraries' Working Group
- BIC / CILIP RFID in Libraries Working Group

This document is not intended to be a specific technical implementation description. Such a document would need to be developed by the international library community to enable library vendors to implement the suggested features contained herein. The purpose of this document is to outline an essentially philosophical approach to the task but with a sufficient level of detail that a technical specification might be developed or evolved from it.

Introduction

Background

There has been much interest in Australia and New Zealand in standards that might be suitable for library-specific RFID systems. In the area of ICTs, libraries have long recognised the value of open systems and the benefits they confer in terms of interoperability. Although systems based on the standard ISO/IEC 15693 have been available to ANZ libraries for some time, the level of awareness existing within most libraries regarding the specific advantages and limitations of this standard has remained low.

Library professionals are often surprised to learn that purchasing a system that is based on this standard (or ISO/IEC 18000-3 Mode 1 of which the standard is a perfect subset) does not guarantee interoperability with other systems based on the same standard. The reason, of course, is that these standards do not mandate a specific format for the data contained within the RFID tag. Library vendors are free to choose any formatting method that they feel will be suitable for their particular system. Therefore, while the RFID tags themselves conform to a standard that describes the manner and method of their communication with an RFID reader, the format of the data written to the tag will almost certainly be different in every vendor's RFID solution.

A considerable level of concern exists regarding this situation, both within the libraries of Australia and New Zealand as well as globally. Several working groups have been formed to consider appropriate methods to overcome this interoperability problem by proposing a specific format for the data on the RFID tag. Some of these initiatives have had a national focus while others have taken a global perspective. The proposal by the Danish group, mentioned earlier, has been accepted as a draft National Standard and has been offered as an appropriate framework for an International standard.

An Australian working group has been formed under the auspices of Standards Australia to examine this proposal as well as others and to develop a suitable model for libraries in Australia and New Zealand. This document reports on the conclusions of the working group.

Working Group

A working group of library and publishing industry professionals was assembled during July of 2005. The members are:

- Alan Butters – Principal Consultant – Sybis (Chair)
- Brian Dunne – Senior Technical Specialist – 3M Australia Pty Ltd
- Jan Wild – Sales Manager ANZ – DA Library Technologies
- Craig Anderson – Director, University Library – RMIT University
- Peter Dart – Information Services Director – Pearson Australia Group
- Christine Mackenzie – Chief Executive Officer – Yarra Plenty Regional Library
- Lynn Regan – Manager, Library Services – Baulkham Hills Shire Council

- Leona Jennings – Coordinator, Library Services Management Projects – Gold Coast City Council
- Janifer Gatenby – Strategic Analysis – OCLC PICA (corresponding member)

The first meeting of the working group took place on September 8th 2005.

Standards

While no specific standard exists for RFID within the library application, a number of standards that could be usefully incorporated into RFID library systems are available and some of these are briefly described below.

ISO/IEC 18000-3 Mode 1
This is an "air interface" standard for RFID systems operating at 13.56 MHz and is the one most commonly used by current library RFID vendors (together with the older ISO/IEC 15693). This standard essentially describes how communication between the RFID tag and the RFID interrogator will take place. While ISO/IEC 15693 was conceived as a smart-card standard, vendors worldwide quickly came to the realisation that it could be easily adapted to a smart-label application (Paret 2005). As previously stated, it does not specify the format of the RFID data placed on a compliant tag. If compliance with ISO standards is claimed by a library RFID vendor, typically the claim references one or both of these two standards.

ISO/IEC 15961 & ISO/IEC 15962
The use of these standards will be considered later in this document but the working group is not aware of any vendor that currently employs these standards as part of their library RFID offering.

ISO 15511
This standard specifies a scheme for uniquely identifying library organisations using International Standard Identifiers for Libraries and Related Organisation (ISIL) codes. Within Australia, the National Library is the managing authority for ISIL. Most Australian libraries already have a NUC code for resource sharing purposes. This can easily be expressed in the form of an ISIL by adding the country code. An infrastructure already exists through the Australian Interlibrary Resource Sharing Directory for a collecting agency without a NUC code to apply for one.

Approach to the Data Model

The following comments reflect at least to some extent the pragmatic position taken by the working group in its approach to the proposals already tabled by existing working groups, particularly that of the Danish group. Never far from the mind of the working group was the desirability, not just of developing another national data model but for a data model flexible enough to serve the needs of the international library community.

Architecture

Before consideration may be given to the individual data elements to be written to the tag, a decision regarding the broad architecture of the data model is required. The key considerations that guided the thinking of the working group during the discussions of possible architectures were:

- Ability of the model to provide maximum flexibility for library sectors as well as individual library organisations
- Ability of the model to cope with change within the RFID industry as the technology develops
- Issues regarding data security and borrower privacy
- The size of the tag memory required
- The quantum of work required for library vendors to implement the model
- The long term desire of libraries to achieve fully open RFID systems
- The use of existing standards within the data model proposal

An analysis of the current data model proposals reveals a preponderance of what could be described as "prescriptive" data models. These models are based on an architecture that offers a "package" of mandatory data elements which must be present on every tag and then another "package" of data elements that can be optionally included or not as a group. In current proposals, these are called the mandatory part and the optional or structured-extension part. A further unstructured area may also be provided, the format of which is left unspecified. The Danish, Finnish, and Dutch models are of this basic architecture.

One of the advantages of such models is that they are relatively easy to implement by library vendors and readily understood by library professionals and other non specialists. However, the working group concluded that these prescriptive models contained significant limitations which make them unsuitable for the long term requirements of libraries, particularly in a global context. Some of those limitations are considered next.

Basic approach
Implicit in the mandatory section of a prescriptive data model is the assumption that the data elements selected will be required by everyone. While these elements are selected with care and following extensive consultation, one truism born of experience remains: Whenever data elements are made mandatory, disagreements will result. In the case of the Danish proposal there are eight mandatory data elements and a package of seven further data elements which may be used as a set. It is easy to imagine a scenario where a library prefers either a different set of elements or perhaps

fewer elements than are contained in the mandatory part. Indeed, the Finnish proposal is a variation of the Danish proposal where this has occurred – one new data element is required whereas others are not to be used.

The working group was concerned that the use of the prescriptive architecture would lead to multiple slightly-differing versions of the same "standard" with progressively reduced interoperability.

Privacy

Of concern to libraries everywhere is the protection of borrower's information. Particularly in the United States have we seen the introduction of RFID systems and reduced borrower privacy closely associated. Calls have been made to keep RFID out of public libraries (EFF, 2005; O'Connor, 2005), to have the State regulate RFID (Mather and Wiebell, 2005), and to postpone the purchase of RFID until privacy issues are solved (Ayre, 2005). There has also been much debate about what is and is not possible to achieve in the tracking, profiling, and spying on individuals due to the library materials they carry.

The working group discussed at length the concerns related to privacy in the context of library RFID and how a data model proposal might be sensitive to these. While acknowledging that an effective approach to privacy and data security must go well beyond a technical solution and deal with the organisational and social issues involved, the working group were keen to acknowledge privacy concerns in the structure of the data model proposal.

A simple measure that can be easily put in place is to reduce the amount of data stored on the RFID tag to the minimum required to circulate the item. Accordingly, one approach that has been recommended is to put only the library item identifier on the RFID tag (Ayre, 2005). While potential functionality might be reduced by such an approach, it does limit the information available to a potential adversary. The working group felt it important that, in this context, libraries should be able to make their own decision regarding what data might be stored on the tag. Clearly, a prescriptive model that mandates multiple data elements for the RFID tag would not easily allow this choice to be made.

Performance

Systems designed to operate with a mandatory part containing several data elements are generally designed to read the entire "package" of data whenever the tag is read. The larger the mandatory part becomes (perhaps due to additional data elements being required as libraries implement RFID using the prescriptive model), the longer it will take to read. Within the Danish Proposal, a Cyclic Redundancy Check (CRC) is included over the entire mandatory block thus indicating that the reading of this whole part will be the standard operation. If the structured extension part is used, an additional set of data elements is generally required to be read. Clearly, a model which offered more flexibility regarding individual data elements rather than "packages" of elements could, under certain circumstances, offer enhanced performance which may be of increased importance within future library applications.

Tag memory usage
One characteristic of RFID tags when compared with other electronic and computer devices is the relatively tiny amount of user memory that they carry. Increased memory capacity means increased cost. Mandating data elements in "packages" limits the way that the small amount of memory existing within the RFID tag may be used.

Long term objectives
While the models proposed to date address the immediate critical need for interoperability at the tag level, they don't really pave the way for the use of standards at higher levels – something essential along the road toward open systems. Current standards do exist which could eventually result in interoperability at higher levels within the RFID architecture such as between the application and interrogator. Interoperability at this level would move the state-of-the-art a long way toward the library utopia of being able to mix and match products from a range of vendors.

Scope

The working group made the decision to consider the wider issues rather than simply the immediate concern of tag-level interoperability. Accordingly, the group didn't feel that item security and the various methods of achieving it could be left beyond the scope of its deliberations. Clearly, libraries want a complete and working solution, including RFID-based security in many instances. Work is proceeding toward the allocation of an "Application Family Identifier" (AFI) for RFID tags attached to circulating library items. This identifier, located in the tag's system memory area is designed to allow other non-library RFID systems using the same international standards to determine that library items with attached RFID tags may be safely ignored by the non-library system.

A scenario where this might be important could exist in a retail outlet with RFID tagged merchandise. In this case, the AFI within the tags attached to library items would enable the retail RFID system to discriminate between library items and local merchandise items. Given that this work is proceeding and expected to be successful, it represents an excellent opportunity for libraries to use this AFI value as part of an item security methodology which would then be common to standardised RFID library systems globally.

The working group also considered the needs of the publishing and retail industries and how the needs of these sectors might impact on a data model proposal.

Conclusions

The working group, while not comfortable with prescriptive data models, acknowledges the extensive work that has been done around the world. The Danish Data Model for Libraries group particularly has produced significant work and the group felt that much could be learned from their proposal document, especially in the selection of data elements. The ultimate proposal was considered by the working group to be a set of similar data elements framed by a different architecture.

Paul Chartier, principal of Praxis Consultants has suggested that the use of two additional standards - ISO/IEC 15961 & ISO/IEC 15962, producing a highly flexible object-oriented architecture might be appropriate. It should be acknowledged that the full implementation of these standards is a more complex project than that of defining a simple model leading only to tag-level interoperability such as those proposed to date. The working group was very much aware that there exists a need for realism when defining a data model proposal as the commercial RFID vendors are the ones who must implement the proposal for it to be successful. However, it was felt that these two new standards offered such an overwhelming advantage for the future of library RFID that this option could not be dismissed. Specifically, the working group concluded that such an approach offered the following benefits:

- Highly flexible architecture
- Single element mandatory part
- Foundation for higher-level interoperability
- Incorporation of existing standards into the architecture
- Good use of tag memory

The use of these standards provides not only a way to deliver a common data model but also offers the possibility of interoperability at the RFID component level. This is a highly desirable outcome for libraries and is a significant move toward a truly open RFID systems architecture. Having made this point, the working group recognise that for commercial reasons, not all RFID vendors might embrace this increased level of interoperability, perhaps fearing that this might lead to loss of differentiation in the marketplace. With this in mind, the working group is proposing an optional two stage implementation:

Stage one
An implementation that provides a data structure on the tag which conforms to the standards but does not require the vendor to implement ISO/IEC 15961 at the application level. In this way, interoperability will not be achieved at the component level but a common tag data model will be delivered. The foundation, however, for a move to a full implementation will be laid.

Stage two
A complete implementation including ISO/IEC 15961 at the application level. This will enable libraries to select components from various vendors to assemble into a system that best suits their needs.

The next section proposes an outline of a data model based on the above conclusions.

Data Model Proposal

Overview

The proposed data model makes use of two international standards which work together to define a data protocol and that will be briefly described. These standards contain many functions highly useful in building an open-systems architecture for library RFID applications. Some of these include:

- Ability to employ an optional directory structure relating to the tag data
- Schemes to uniquely identify library data within the global RFID application space
- Data formatting and compaction
- Support for fixed and variable fields
- Object locking
- Ability to selectively read objects from the tag
- Ability for the data model to be used on multiple RFID platforms
- Complete flexibility regarding which data elements to employ
- Compatibility with different tag memory capacities

The two standards in question are:

- ISO/IEC 15961
- ISO/IEC 15962

ISO/IEC 15961 is a data protocol that specifies how data will be exchanged between the application (which in the current context could be the library's information management software and databases) and the data protocol processor which would most often be a component contained within the RFID interrogator device.

The standard defines an object-oriented approach to identifying the data elements and specifies the commands necessary to move data into and out of the application and to append, update or delete data on the RFID tag. The protocol also includes appropriate error messages that can be sent to the application.

ISO/IEC 15962 specifies common encoding rules for data to be placed on the RFID tag as well as logical memory functions inside the data protocol processor of the RFID interrogator device. The standard includes a scheme whereby data elements can be processed as data objects with unique identifiers. These object identifiers ensure that the data object is not only unique within the library application of RFID, but also unique within all other RFID applications conforming to the standard.

In order to conserve space on the RFID tag, only *relative* object identifiers (OID) are stored by use of the data formatter which is part of the ISO/IEC 15962 standard. The relative OID refers to the final node of the object identifier and assumes that all of the previous nodes in the object identifier are the same for every object which will be true in the case of all RFID tags used within the library application. A useful analogy to aid understanding of this would be the physical address of an apartment block. Once the Country, State, City, Street name and Street number are known, a single apartment number then identifies every individual apartment. For a known address, the

apartment numbers could be considered as relative identifiers for each occupant and indeed are used as such by the tenants, for example "Mr Smith in apartment 6", and so on. Within the apartment building, it is not necessary to use the full form of the address.

While the object identifier structure has not yet been assigned for libraries, it is expected that this will shortly take place as part of the process for obtaining an Application Family Identifier (AFI) for on-loan items (see section on item security). Using relative object identifiers in the range from 1 to 14 ensures that the relative OID's are encoded efficiently as part of the precursor octet (see ISO/IEC 15962 – section 8.3, Data Formatting for more detail). It is recommended that the most useful and most used data elements are therefore assigned to relative OIDs between 1 and 14. More elements may be defined (OIDs 15 to 127) but their use will add an extra octet for the encoding.

While use of a directory structure is included in the standards, it is not used in this proposal.

Data Elements

The following table of data elements is proposed for relative object identifiers 1 to 11. It is not meant to be exhaustive and indeed the expectation is that it may be expanded, a situation for which the standards allow, as previously stated. The order presented is based on the placement of the most commonly used elements first.

Data Element	ISO 8459 mapping	Rel. OID	Category	Format	Lock
Primary item ID	Copy Identifier	1	Mandatory	Variable length Alphanumeric	O
Owner institution	Party Identifier & Participant's func.	2	Optional	Variable length field based on ISO 15511	O
Type of usage	-	3	Optional	Single octet fixed length field	O
Usage Qualifier	-	4	Optional	Single octet fixed length field	O
Set Information	Number of Volumes	5	Optional	Two octet fixed length field	Y
Media Format	Format of item (technical specs)	6	Optional	Single octet fixed length field	O
Item title	Title	7	Optional	Variable length Alphanumeric	O
Secondary item ID	Copy Identifier	8	Optional	Variable length Alphanumeric	O
Supplier ID	Party Identifier & Participant's func.	9	Optional	Variable length Alphanumeric	O
Invoice Number	Invoice Identifier	10	Optional	Variable length Alphanumeric	O
Order Number	Request Identifier	11	Optional	Variable length Alphanumeric	O

Description

Data Element	Rel. OID	Category	Format	Lock
Primary item ID	1	Mandatory	Variable length Alphanumeric	O

This element is the primary identifier for the item, often but not necessarily equivalent to the library barcode. While the primary identifier will be often 14 characters or less, identifiers have been observed internationally up to 27 characters. By use of the compactors contained within the standards, only the actual space required for the specific item identifier is used on the RFID tag, regardless of length. Shorter item identifiers will consume less memory on the tag than longer ones. The lock-field parameter has been left optional, however under normal circumstances this data element might be locked to prevent various forms of digital vandalism.

It is strongly recommended that the Primary Item ID be assigned the first relative object identifier and that the object always be encoded in the first position on the RFID tag. This allows the use of the *Read First Object* command module within ISO/IEC 15961 in applications where only the item identifier is required and speed of reading is a critical factor.

Data Element	Rel. OID	Category	Format	Lock
Owner institution	2	Optional	Variable length field based on ISO 15511	O

This element represents the ISIL code according to ISO 15511. The hyphen is present in every ISIL code following the two-character country code and so this hyphen is not stored on the RFID tag but is recreated by the application software after the data is read by the interrogator. The use of these codes assumes an external Inter Library Loans (ILL) system capable of tracking the item based on the unique combination of its Primary Item ID and Owner Institution. It is considered to be infeasible at this stage to manage the entire ILL transaction by means of only the data stored on the RFID tag. This element is optional where items are not included in an ILL scheme but required when items are issued on ILL. While it may be deemed necessary to lock this data element, it has been left optional as some libraries may choose to leave it unlocked so that it could be changed if necessary as a result of library mergers or transfer of collections etc.

Data Element	Rel. OID	Category	Format	Lock
Type of usage	3	Optional	Single octet fixed length field	O

This element defines whether the RFID tag corresponds to an *item* within the library or a *user* of the library. This allows for the situation where a library uses an RFID tag to identify library borrowers as part of a membership card. If the tag corresponds with a library item, the element defines the type of material and its use within the library. It can also signal that special handling may be required such as when automated sorters

are used. As synergies between RFID enabled devices become more common, this element may be set dynamically by one RFID device for the benefit of another. A number of values are reserved for local use. These could be ignored where the Owner Institution is not that of the processing library (as in ILL). 256 values are permissible, some structure may be desirable and the following is suggested as an example:

Range	Class	ID	Usage
1–32	Borrowers	1	Standard Library Users
33-42	Item Status	33	Circulating item
		34	Non circulating item
		35	Discarded item
43-52[1]	Special handling codes	43	Special handling code 1
		44	Special handling code 2
		45	Special handling code 3
52–71[2]	Library equipment	52	Library equipment code 1
		53	Library equipment code 2
		54	Library equipment code 3
200-255	Special internal use		Defined and employed locally

Notes:

1. These codes may be defined locally and are intended to convey specific item information to automatic sorters where special handling is required due to the item's size or other properties etc.
2. These codes are intended to identify library equipment that may be on loan or reserved for use by borrowers within the library.

Data Element	Rel. OID	Category	Format	Lock
Usage Qualifier	4	Optional	Single octet fixed length field	O

This data element may be used in combination with the "Media Format" or "Type of Usage" elements to allow further flexibility when processing library items. There are alternative viewpoints within the working group regarding this data element and the advantage it confers. It has been suggested that with only a single "Type of Usage" parameter, some situations where usage types are not mutually exclusive may not be provided for. The example given is a situation where a particular item may require a different status when being issued than when it is returned, perhaps not be circulated through self serve loans AND requiring special handling when being returned.

Obviously this situation could be covered by a single "Type of Usage" designator but concern was expressed that there may be many of these sorts of cases and that a very long list would be needed to cover every eventuality whereas the ability to combine two fields would be more easily managed. Input from the broader library community

is required to determine of this element is valuable and if so, how it might be best formatted. 256 values are permissible and some structure may be desirable.

Data Element	Rel. OID	Category	Format	Lock
Set Information	5	Optional	Two octet fixed length field	Y

This data element contains two parameters which are stored together.

- Parameter 1 = Number of items in set
- Parameter 2 = Number of this item

These two combined parameters are used to identify the many permutations relating to material sets. The first parameter indicates the number of items that exist in the set (up to 256). The second parameter is used to identify each item within the set. If the second parameter is set to 0, this indicates that the set has only a single RFID tag. Otherwise where multiple items in the set have individual RFID tags, the second parameter indicates the number of the item within the set. Please refer to the following examples:

Example 1:
A set consisting of a single item with one RFID tag:
Number of items in set = 1
Number of this item = 1

Example 2:
A set with three items, all with their own RFID tags:
Number of items in set = 3
Number of this item = 1 (first RFID tag)
Number of this item = 2 (second RFID tag)
Number of this item = 3 (third RFID tag)

Example 3:
A set having three items but only one RFID tag for the whole set:
Number of items in set = 3
Number of this item = 0

Data Element	Rel. OID	Category	Format	Lock
Media Format	6	Optional	Single octet fixed length field	O

This element represents an ONIX media descriptor. 256 values are possible, the following values are established:

Value	ONIX Value	Description
0	00	Undefined
1	AA	Audio
2	AB	Audio cassette
3	AC	CD-Audio

4	AD	DAT
5	AE	Audio disk
6	AF	Audio tape
7	AG	MiniDisc
8	AH	CD-Extra
9	AI	DVD Audio
10	AJ	Downloadable audio file
11	AZ	Other audio format
12	BA	Book
13	BB	Hardback
14	BC	Paperback
15	BD	Loose-leaf
16	BE	Spiral bound
17	BF	Pamphlet
18	BG	Leather / fine binding
19	BH	Board book
20	BI	Rag book
21	BJ	Bath book
22	BK	Novelty book
23	BL	Slide bound
24	BM	Big book
25	BZ	Other book format
26	CA	Sheet map
27	CB	Sheet map, folded
28	CC	Sheet map, flat
29	CD	Sheet map, rolled
30	CE	Globe
31	CZ	Other cartographic
32	DA	Digital
33	DB	CD-ROM
34	DC	CD-I
35	DD	DVD
36	DE	Game cartridge
37	DF	Diskette
38	DG	Electronic book text
39	DH	Online resource
40	DI	DVD-ROM
41	DZ	Other digital
42	FA	Film or transparency
43	FB	Film
44	FC	Slides
45	FD	OHP transparencies
46	FE	Filmstrip
47	FF	Film
48	FZ	Other film or transparency format
49	MA	Microform
50	MB	Microfiche
51	MC	Microfilm

52	MZ	Other microform
53	PA	Miscellaneous print
54	PB	Address book
55	PC	Calendar
56	PD	Cards
57	PE	Copymasters
58	PF	Diary
59	PG	Frieze
60	PH	Kit
61	PI	Sheet music
62	PJ	Postcard book or pack
63	PK	Poster
64	PL	Record book
65	PM	Wallet
66	PN	Pictures or photographs
67	PO	Wallchart
68	PP	Stickers
69	PZ	Other printed item
70	VA	Video
71	VB	Video, VHS, PAL
72	VC	Video, VHS, NTSC
73	VD	Video, Betamax, PAL
74	VE	Video, Betamax, NTSC
75	VF	Videodisk
76	VG	Video, VHS, SECAM
77	VH	Video, Betamax, SECAM
78	VI	DVD video
79	VJ	VHS video
80	VK	Betamax video
81	VL	VCD
82	VM	SVCD
83	VZ	Other video format
84	WW	Mixed media product
85	WX	Quantity pack
86	XA	Trade-only material
87	XB	Dumpbin – empty
88	XC	Dumpbin – filled
89	XD	Counterpack – empty
90	XE	Counterpack – filled
91	XF	Poster
92	XG	Shelf strip
93	XH	Window piece
94	XI	Streamer
95	XJ	Spinner
96	XK	Large book display
97	XL	Shrink-wrapped pack
98	XZ	Other point of sale
99	ZA	General merchandise

100	ZB	Doll
101	ZC	Soft toy
102	ZD	Toy
103	ZE	Game
104	ZF	T-shirt
105	ZZ	Other merchandise

Data Element	Rel. OID	Category	Format	Lock
Item title	7	Optional	Variable length Alphanumeric	O

This is a variable length field. It is recommended that all uppercase characters be used in the title as this encodes more efficiently. In situations where tag memory is small, a locally defined and administered limit could be placed on the length of this field. The length should be the shortest that is practical to satisfactorily identify the item (from a small set of items, for example one item from six as a library borrower exits the security gates and triggers an alarm due to a processing error).

Data Element	Rel. OID	Category	Format	Lock
Secondary item ID	8	Optional	Variable length Alphanumeric	O

This is a variable length field that may be used for a locally designated optional ID. The ID may be temporary and have only local meaning as during an acquisitions process or it may contain codes such as ISBN etc.

Data Element	Rel. OID	Category	Format	Lock
Supplier ID	9	Optional	Variable length Alphanumeric	O

This is a variable length field that may be used for a locally designated identification number relating to the supplier of the library material. It may be left permanently written to the tag or it may be used only temporarily during an acquisitions process.

Data Element	Rel. OID	Category	Format	Lock
Invoice Number	10	Optional	Variable length Alphanumeric	O

This is a variable length field that may be used for a locally designated invoice number meaningful to the library and to the supplier of the library material. It may be left permanently written to the tag or it may be used only temporarily during an acquisitions process.

Data Element	Rel. OID	Category	Format	Lock
Order Number	11	Optional	Variable length Alphanumeric	O

This is a variable length field that may be used for a locally designated order number meaningful to the library and to the supplier of the library material. It may be left permanently written to the tag or it may be used only temporarily during an acquisitions process.

Security

While acknowledging that use of the data encoding area of the RFID tag is fundamentally weak for security, many libraries wish to implement item security on an ISO compatible tag. EAS functionality is not supported under ISO/IEC 18000-3 Mode 1 tags. The working group's preference for those libraries wishing to use RFID tag-based security is for a pair of data values to signal the status of the library material and its eligibility to be removed from the secure area. It has been suggested that the AFI value contained in the systems part of the RFID tag could usefully be used for security. The difficulty to date has been that there is not an AFI pair of values (checked-in / checked-out) assigned to libraries. Current indications suggest that a single AFI for on-loan books will be issued in the near future. A closed-system "checked-in" value should be used while the item is on shelf in the library. A standardised closed-system value is available for internal uses such as this and together these values may be used to determine the security status of library items.

Use of the AFI values for security will ensure that a standardised security mechanism is available to all institutions that are performing transactions with the RFID-tagged material. Use of the AFI values for tag-based security does not preclude the use of external mechanisms such as electromagnetic (EM) security systems. If an individual library chose to integrate EM security employing covert security strips into their operation, the AFI value should be left permanently in the on-loan state and ignored for security by the local RFID application. This would still serve the purpose of allowing RFID systems from other application areas to identify the tagged item as library material. If an item possessing both an EM strip and an RFID tag was circulated by a library using only RFID security (such as in cooperative arrangements or Inter-library loans) the library could make use of the AFI values for security while the item was under its control.

The AFI values are:

Application Family Identifier	Status	Usage	Lock
TBA	On-loan	Items on loan to borrowers – unsecured by the RFID tag	N
TBA	Closed system	Items on shelf or for internal use within the library – secured by the RFID tag	N

Privacy

Much has been made of possible attempts to compromise the privacy of library users when a library choses to implement an RFID system to manage their circulating collections. The degree to which these issues exist within a community may determine to some extent what data elements are placed on the RFID tag. The proposed data model acknowledges this by permitting a library to store only the item identifier if so desired.

This, of course, does not prevent some of the tracking, profiling and hotlisting threats that have been raised by some commentators (Lahari, 2006). It has been suggested that to enhance security the library application could generate single-use item identifiers at the point of issue which are paired with the item record within the library database (Molnar and Wagner, 2004). This would ensure that the item circulates with a different identifier for each borrower. Of course such a scheme, if implemented, is outside the scope of this document.

Unfortunately, for a truly secure RFID implementation, ISO/IEC 18000-3 Mode 1 is not an ideal platform. For several reasons, including the fact that the air interface specified by the standard "leaks" the manufacturer's unique tag identifier during collision avoidance exchanges (Molnar and Wagner, 2004), the working group considers that a cryptographically secure and item-anonymous system based on this standard cannot be implemented and is therefore such a system lies outside the scope of this document. More library-centric research is needed in this area. Naturally, each library must give consideration to how, within the limits available to them, they will endeavour to take reasonable precautions in ensuring borrower privacy. These precautions obviously extend beyond the RFID tag and the data it contains and encompass issues relating to process, database, and document storage & control etc.

There is also much that can be said about the non-technical issues associated with data security and privacy. Such social and organisational issues fall outside the scope of this document but must be addressed by the library profession as part of the broader debate. It is anticipated that such things as codes of best practice and operating frameworks will be developed to help individual libraries deal with some of the complex issues involved.

While not always directly relating to privacy, the issue of data security is, as stated above, difficult to address with the currently used ISO/IEC 18000-3 Mode 1 standard. The data model proposal permits the locking of data on the tag, thus preventing future changes to this data. Some libraries may decide to lock all of the tag data whereas others may wish to lock some or no data. In the majority of cases the working group has left the locking or unlocking of data optional. Libraries should give careful thought to their strategy in this area.

One of the benefits of most RFID tags is that they can be re-written a great number of times. As stated previously, there is debate regarding what data the tag should contain when it leaves the library with many libraries electing to place only the minimum data on the tag, as stated previously. We must not forget, however, that library RFID systems may evolve to utilise more fully the re-writable nature of the RFID tags. Perhaps different "profiles" could be developed where tags may have a different

dataset within the library compared to the dataset used when circulating. In this way, internal functionality might be provided without borrower privacy being compromised as the data set would be changed when the items leave the library. The proposed model would accommodate this scenario.

One example of this might relate to storing the item's title in the RFID tag. Useful functionality is provided by this data when the RFID tag is used for item security. If the security gates alarm, a message can be flashed to a staff PC indicating the actual title of the item that has triggered the alarm. This enables one item from many to be quickly identified. Some systems on the market currently offer this functionality. Unfortunately, from a borrower-privacy perspective, having the title stored on the RFID tag is undesirable. The fact that the tag may be rewritten allows for both these scenarios to exist – the title stored while the item is inside the library, and removed from the tag when the item is issued to a borrower. Any unprocessed item leaving the library will still contain the title and can therefore be used for identification when the alarm is triggered.

Inter Library Loans might furnish another example. The issue of borrowers being "profiled" to some extent due to the identity or the location of the borrowing institution contained within the RFID tag has been raised (Molnar and Wagner, 2004). The use of data "profiles" may allow ownership data to exist within the RFID tag only when the material is moved between institutions rather than in every circulating item.

There may be other useful "profiles" associated with acquisitions etc. The point here is that the re-writable nature of the tag may be useful in the future when combined with a flexible and potentially dynamic data model and so in anticipation of this, as a minimum, it may be desirable to maintain an unlocked area on the tag. Libraries are able to weigh the relative pros and cons of such an approach and balance this with the increased level of functionality that may be achieved.

Implementation

It is the collective view of the working group that the long term interests of libraries are likely to be best served by a move toward a truly open RFID systems architecture. With this in mind, the selection of a data model and its implementation should, as a minimum, move the library community toward this outcome. By employing standards at the higher levels within the RFID architecture, this proposal paves the way for such a future while providing excellent flexibility and interoperability in the short term.

As stated previously the working group recognises commercial sensitivities and so suggests that the implementation of this proposal may proceed in two stages. A conceptual scope for each of these stages is detailed below. Note that this is presented at a level of abstraction intended to convey only the principles involved. An acceptance of the two stage approach would lead to the development of a technical document generated in consultation with RFID vendors and which describes precisely where the boundary between the stages would be created.

Stage one:

The purpose of this stage is to provide an appropriate data structure on the RFID tag that complies with the structure generated according to ISO/IEC 15961 and ISO/IEC 15962 but that may be accomplished by the vendor using proprietary methods. The implementation task should therefore be smaller and there is no requirement at this stage to inject standardisation at the application level. The requirement is to ensure a tag data format that will remain unchanged when full standardisation (in Stage 2) is implemented at a point in the future. Specifically, this means:

The Application Family Identifiers must be set according the this proposal for circulating material
The data objects must be formatted to be compatible with ISO/IEC 15961 and ISO/IEC 15962 and their relative OIDs set as per this document.
The encoding and compaction method to be compatible with ISO/IEC 15961 and ISO/IEC 15962

Stage two:

This is a complete implementation of ISO/IEC 15961 and ISO/IEC 15962. The standardisation at this level achieves the open-systems outcome that libraries seek, allowing them to discriminate between vendor's products at the component level.

Examples of data model options

The following combinations illustrate possible scenarios that might be chosen by a library and the memory requirements for each following encodation onto the RFID tag. It should be noted than a minimum implementation with an RFID tag containing the primary item ID is easily possible under this proposal where tags with only 256 bits of memory (32 bytes) are used. This is considered to be the smallest memory capacity in current systems – many tags currently used have significantly larger memory capacities. Some assumptions are made in these examples which are based on commonly seen values. All values are in bytes. An additional 3 bytes overhead is assumed for locked primary item ID and typical Owner Institution (ISIL) code.

Minimum implementation

Data Object	Length	Overhead	Sub Total
Primary Item identifier (typical 14 numerics)	7	5	9
		Total	**12**

Worst-case minimum implementation (longest barcode observed)

Data Object	Length	Overhead	Sub Total
Primary Item identifier (27 characters)	24	5	29
		Total	**29**

Minimum Inter Library Loans implementation

Data Object	Length	Overhead	Sub Total
Primary Item identifier (typical 14 numerics)	7	5	12
Owner Institution (typical)	7	2	9
		Total	**21**

Typical implementation

Data Object	Length	Overhead	Sub Total
Primary Item identifier (typical 14 numerics)	7	5	9
Owner Institution (typical)	7	2	9
Type of usage	1	2	3
Media Format	1	2	3
		Total	**24**

Typical implementation where the tag is attached to a set

Data Object	Length	Overhead	Sub Total
Primary Item identifier (typical 14 numerics)	7	5	12
Owner Institution (typical)	7	2	9
Type of usage	1	2	3
Media Format	1	2	3
Set Information	2	2	4
		Total	**31**

Next Steps

A major decision to be made by libraries internationally relates to the question of what we want to accomplish in the long term with regard to RFID. If our horizons extend to only achieving interoperability at the tag level, then a prescriptive model will suffice. If we want interoperability in the short term but desire an open RFID systems architecture as an end goal, then we must standardise more than simply the tag data model.

Standards already exist to allow us to accomplish this. With a little extra effort and a clear vision for the future, we can pave the way for the RFID systems of tomorrow. If we fail to engage with that future now, we will certainly need to do so at some time in the future and therefore our interim prescriptive model will make way for one based on international standards. The Standards Australia IT-19-01-02 working group is suggesting that we begin as we aim to proceed and adopt an approach to standardisation that will deliver the long term benefits that libraries require.

The proposal contained in this document needs to be studied, challenged and evaluated. If the philosophical approach is deemed to be sound, then what remains is the task of ensuring that the particular expression of that approach is valid before moving forward. Once a decision is made to proceed down a standards-based path, the detail can be determined and agreed-upon by consultation and negotiation. From a final specification document a technical implementation outline can be developed to ensure that library RFID vendors have a clear and unambiguous path before them.

Historical precedents would suggest that a standardised approach leaving competition to occur along lines of product features and benefits will be in the best interests of libraries *and* vendors over the long term.

References

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/

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

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

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, 111-220