NISO RP-6-2008

RFID in U.S. Libraries

December 2007

A Recommended Practice of the
National Information Standards Organization

Prepared by the
NISO RFID Working Group

About NISO Recommended Practices

A NISO Recommended Practice is a recommended "best practice" or "guideline" for methods, materials, or practices in order to give guidance to the user. Such documents usually represent a leading edge, exceptional model, or proven industry practice. All elements of Recommended Practices are discretionary and may be used as stated or modified by the user to meet specific needs.

This recommended practice may be revised or withdrawn at any time. For current information on the status of this publication contact the NISO office or visit the NISO website (www.niso.org).

Published by
National Information Standards Organization (NISO)
One North Charles Street, Suite 1905
Baltimore, MD 21201
www.niso.org

Printed in the United States of America
ISBN (10): 1-880124-75-0
ISBN (13): 978-1-880124-75-8

Table of Contents

Foreword ..... **iv**

Summary of Recommendations ..... **viii**

Section 1: Use of RFID in Libraries **1**

1.1 Overview 1
1.2 Tagging in Libraries 1
1.3 Self Check-Out 2
1.4 Check-In, Including Manual, Conveyor, and Sorting Systems 2
1.5 Inventory Systems 3
1.6 Support for Interlibrary Loan (ILL) 3
1.7 RFID Standards in Libraries 3

Section 2: NISO Data Model **5**

2.1 Introduction 5
2.2 Data Objects 5
2.2.1 Advantages of Looking Up Data in the ILS 6
2.2.2 Advantages of Storing Data on the Tag 6
2.3 Mandatory and Optional Data Objects 6
2.4 Locked vs. Unlocked 7
2.5 Data Model 7
2.5.1 Primary Item ID 9
2.5.2 Tag Content Key (also called OID Index) 9
2.5.3 Owner Library/Institution 10
2.5.4 Set Information (also called “multi-part indicator”) 10
2.5.5 Media Format 11
2.5.6 Type of Usage 11
2.5.7 Shelf Location 11
2.5.8 ILL Borrowing Institution 12
2.5.9 ILL Transaction ID 12
2.5.10 GS1 Identifier (includes ISBN) 13
2.5.11 Title 14
2.5.12 Supply Chain Stage 14
2.5.13 Supplier Item ID (Alternate Item ID) 15
2.5.14 Local Data –1 15
2.5.15 Local Data –2 16
2.5.16 Order Number 16
2.5.17 Invoice Number 16
2.5.18 Supplier Identification Data 16
2.6 Relative OID 17
2.7 Encoding 17

2.8 Use of Primary IDs and Supply Chain Stages 18
2.9 Comparison Between NISO Data Model and Australian Data Model 19

Section 3: Security **20**

3.1 RFID Security for Libraries 20
3.2 AFI 20
3.2.1 AFI Codes and Interoperability 21
3.2.2 AFI Locking 21
3.2.3 Interlibrary Loan Situations 21
3.3 Electronic Article Surveillance (EAS) 22
3.4 Virtual Deactivation (Database Look-Up) 22
3.5 Recommendations for Security 23

Section 4: Migration to ISO Standard Tags **25**

4.1 Introduction 25
4.2 User Considerations in Upgrading 27
4.3 Role of RFID Vendor 27
4.4 Suggested Migration Process 27
4.5 Libraries Currently Considering the Purchase of an RFID System 28
4.5.1 Emerging Technologies 29

Section 5: The Book Supply Chain **31**

5.1 Introduction 31
5.2 Book Supply Chain Overview 31
5.3 RFID in the Supply Chain 33
5.4 Book Jobbers and RFID Tag Application 34

Section 6: Privacy **37**

6.1 Privacy Issues 37
6.2 EFF Position on RFID and Personal Privacy 38
6.3 ALA/BISG Initiative 38
6.4 A Technology Perspective on Privacy Concerns 39

Section 7: Vandalism **41**

7.1 Introduction 41
7.2 Modification of Security Data 41
7.3 Modification of Tag Contents 42
7.4 RFID Viruses 42
7.5 Physical Defacing or Removal of the Tag 42

7.6 Intentional Detuning of the Tag 43
7.7 Moving Forward 43

Appendix A: RFID Technology Basics 44

Appendix B: Interoperability Characteristics 51

Appendix C: Comparison of USA-NISO and Australian Data Models 54

Appendix D: Codes for Media Format 55

Appendix E: Encoding Data on the RFID Tag 59

Glossary 76

Bibliography 77

Foreword

NISO RFID Working Group Charge

The NISO RFID Working Group was formed to focus on the use of radio frequency identification (RFID) technologies in U.S. libraries. As our work has moved forward, however, there have been new developments with regard to RFID implementation in the larger book industry as well as in other countries, including the U.K., Denmark, the Netherlands, and Australia. Indeed, RFID technologies are still evolving and thus represent a moving target. As a result, it is important to understand the needs of the several elements of the publishing value chain, especially as concerns standards and interoperability.

Among the goals of our work are the following:

1) To review existing RFID standards, assess the applicability of this technology in U.S. libraries and across the book publishing supply chain, and promote the use of RFID where appropriate.
2) To examine and assess privacy concerns associated with the adoption of RFID technologies in libraries.
3) To investigate the way RFID may be used for the circulation or sale of books and other media in the United States and make recommendations.
4) To focus on security and data models for RFID tags, along with issues of interoperability and privacy.
5) To create a set of recommendations for libraries with regard to a tag data model and other issues.

To achieve these goals, we recognized the need to involve a broad spectrum of book industry participants, including:

- librarians (academic & public),
- RFID solution providers (software and integration),
- RFID hardware manufacturers,
- book jobbers and distributors,
- publishers, and
- book manufacturers and printers.

The charge of this working group was *limited to item identification*—that is, the implementation of RFID for books and other materials—and specifically *excludes* its use with regard to the identification of people. Thus, this report does not touch on the subject of smart cards and other uses of RFID for the identification of individual persons. The NISO RFID Working Group specifically recommends that data relating to individual persons never be recorded on item tags.

Ideal Outcome

The NISO RFID Working Group charge is a difficult one. Ideally, the best outcome would be one that achieves true interoperability, perhaps even at the international level, while protecting personal privacy, supporting advanced functionality, facilitating security, protecting against vandalism, and allowing the RFID tag to be used in the entire lifecycle of the book and other library materials.

These NISO recommendations for best practices should promote procedures that:

- Allow an RFID tag to be installed at the earliest point in the lifecycle of the book and used throughout its lifecycle from publisher/printer to distributor, jobber, library (shelving, circulating, sorting, re-shelving, inventory, and theft deterrence), and interlibrary loan and then on to secondary markets such as secondhand books, returned books, and discarded/recycled books.
- Allow for true interoperability among libraries; that is, a tag in one library can be used seamlessly by another, even if they have different suppliers for tags, hardware, and software.
- Protect the personal privacy of individuals while supporting the functions that allow users to reap the benefits of this technology.
- Permit the extension of these standards and procedures for global interoperability.
- Remain relevant and functional with evolving technologies.

The outcomes mentioned above may not be fully achievable. However, we cannot ignore the issues, for they will not go away, nor will they resolve themselves without cooperation and mutual understanding.

Early and current RFID implementers are at considerable risk because of the lack of interoperability of proprietary vendor systems. While some movement toward interoperability is occurring, true interoperability that allows libraries to procure the tags, hardware, and software from independent providers and book jobbers to use with all tags is still a long way from reality.

An RFID standard with an agreed upon data model is an essential first step. While a data model cannot fully resolve the interoperability issue, it offers a giant initial step by defining fields that are either mandatory or optional and either locked or unlocked for library applications. This model is a key precursor to a world in which a library can procure tags from different vendors, merge collections containing tags from different vendors, and, for the purposes of interlibrary loan, read the tags on items belonging to other libraries.

Even with a data model, there are other barriers to interoperability and plug-and-play capabilities. They include:

1) vendor-specific encrypting and encoding of the data;
2) proprietary security functions, which are an advantage when considering hackers, thieves, etc., but are a detriment to interoperability (see Section 3); and
3) software or firmware that are system dependent and can only be used with specific tags.

In a nutshell, even a tag that conforms to the data model may not currently work with another vendor's equipment. But, the future is not all bleak. With standards either developed or under development to cover most aspects of RFID technology, library customers demanding interoperability, and the movement toward embedding tags into books at manufacture, it is only a matter of time until systems will be truly interoperable.

For libraries already heavily invested in RFID, Section 4 addresses issues related to migration or upgrading of tags to be compliant with the data model.

In this report, The NISO RFID Working Group is providing its best insights into these complex issues and a possible way forward.

NISO Topic Committee Members

The Content and Collection Management (CCM) Topic Committee had the following members at the time it approved this Recommended Practice:

Julia Blixrud
Association of Research Libraries (ARL)

Kevin Cohn
Atypon Systems Inc.

Ted Fons
Innovative Interfaces, Inc

Juha Hakala
The National Library of Finland

Diane Hillmann
Cornell University Library

Ted Koppel (Chair)
Consultant

Katherine Kott
Stanford University Libraries & Academic Information Resources

Rollo Turner
Association of Subscription Agents (ASA)

Bonnie Lawlor
National Federation of Advanced Information Services (NFAIS)

Denise Troll Covey
Carnegie Mellon University Libraries

NISO RFID Working Group Members

The following individuals served on the NISO RFID Working Group, which developed and approved this Recommended Practice:

Livia Bitner
Baker and Taylor

Vinod Chachra (Chair)
VTLS Inc

Brian Green
EDItEUR

Jim Lichtenberg
Book Industry Study Group

Alastair McArthur
Tagsys

Allan McWilliams
Baltimore County Public Library

Louise Schaper
Fayetteville (Arkansas) Public Library

Paul Sevcik
3M Library Systems

Paul Simon
Checkpoint Systems, Inc.

Marty Withrow
OCLC

Acknowledgements

This document gained immensely by a small but dedicated group of reviewers who painstakingly read the entire document and suggested several changes. We are grateful to this group of reviewers:

Gretchen Freeman
Salt Lake County Library Services

Margaret E. Hazel
Eugene Public Library

Doug Karp
TAGSYS, Inc.

Corrie Marsh
Hong Kong University of Science & Technology

Rob Walsh
Envisonware

Trademarks, Service Marks

Summary of Recommendations

The key goal of this document is to promote interoperability where RFID systems or products work with other RFID systems or products without special effort or intervention on the part of the customer across the supply chain. This will create institutional and supply chain efficiencies, reduce component cost, and improve return on investment in RFID technologies.

Today we are far from an interoperable environment. Most RFID systems available are proprietary in some manner. Customers currently often purchase tags, readers, self check-out stations, and any other components from the same vendor. The proprietary nature of these systems increases costs, makes changing vendors expensive, results in hesitancy to purchase RFID technologies, and limits the real potential of RFID as a cross-institution platform for identification.

Interoperability is desired in some environments and not in others. For example, library tags should not set off alarms in bookstores and grocery stores and vice versa. It is important that there be vertical application isolation. The application family identifier (AFI—see Section 3) is a key mechanism to control this aspect of operations.

It is recommended that:

1) RFID tags should comply with the ALA/BISG *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles*, [1] in particular, ensuring that data relating to individual persons should never be recorded on item tags.
2) In libraries, 13.56 MHz High Frequency (HF) tags should be used.
3) RFID tags for library use should be “passive” (as opposed to “active”).
4) The read range of tags for library applications should not be substantially increased in future instances beyond the present range. The typical read range today is 8-20 inches for smaller tags and somewhat higher for larger tags.
5) Only tags including a standardized AFI feature should be used in libraries.
6) The AFI byte should be coded to define a tag on any loaned item as belonging to the family called “library applications.” Furthermore, discharged items in libraries using AFI for security should be using an AFI code assigned for those items, as described in Section 3.
7) The security recommendations in Section 3.5 should be followed.
8) In order to help ensure interoperability, security implementations for RFID in libraries should not lock a compliant system into any one security possibility, but rather leave security as a place for differentiation between vendors. (See Section 3 for details)
9) RFID tags should be reprogrammable for migration purposes and libraries should ensure that equipment upgrades that can handle both proprietary and standard formats are made before tags are reprogrammed.
10) Data on RFID tags should be encoded according to the Data Model described in Section 2, using encoding described in ISO/IEC 15962 and using relative object IDs specified in an anticipated ISO standard for RFID in Libraries (ISO/NP 28560).

[1] American Library Association, *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles* (January 19, 2005) http://www.ala.org/ala/oif/statementspols/ifresolutions/rfidresolution.htm

Section 1: Use of RFID in Libraries

1.1 Overview

Libraries use RFID tags on books and other items to provide identification during check-out, check-in, inventory, and for theft deterrence. Benefits of adoption may include:

- reduction of staff manual processes and errors;
- reduction of staff and patron time spent in finding items;
- increased customer satisfaction and access to more items as the fast RFID check-in process quickly clears their accounts; and
- enhanced customer experience through fast and private self check-outs.

While costs continue to decrease due to mass adoption, current RFID implementations require a considerable initial investment and ongoing expense. While there is a dearth of both anecdotal and published reports on return on investment, the rationale for implementation today is based on the following criteria, including:

1) percentage of staff time spent on check-out,
2) percentage of staff time spent on check-in,
3) volume/percentage of check-outs handled by staff versus patrons,
4) increase in check-outs handled without additional staff,
5) speed and accuracy of inventory,
6) accuracy of check-in,
7) worker's compensation costs from repetitive strain injuries, and
8) customer satisfaction with check-out and check-in processes.

1.2 Tagging in Libraries

Early implementers of RFID technology have been obliged to apply and program their own tags to library items, e.g., books, periodicals, media, kits, and other assets. Now libraries may choose to have their book jobbers apply and program tags prior to shipment. While this is an increasing trend for new items, in-library application is still required for retrospective conversions of existing items and new books, media, periodicals, donated materials, and other items not procured through the book jobber. In the longer term, source tagging at item manufacture is likely.

Retrospective conversions can be processed wherever there is a PC with barcode scanner, programming software, and an RFID reader. The conversion procedure is straightforward and should take only a few seconds per item. The task can be performed by non-technical staff or volunteers. Some vendors also offer dedicated tagging and programming stations with touch screens, automated tag dispensing, and portability for in-stack use. Consideration must be given to the cost of dedicated stations and their space requirements.

1.3 Self Check-Out

Self check-out stations are generally proprietary touch-screen devices composed of an RFID reader, barcode scanner for library cards, receipt printer, customer-friendly interface software, and, if the library's integrated library system (ILS) does not offer a self check-out module, NCIP or SIP protocol software to communicate with the library's ILS application or database. Often, these stations allow users to view their library accounts, pay fines, and perform other functions.

It is entirely feasible to procure a generic kiosk and outfit it with an RFID reader, barcode scanner, and necessary software at less expense and possibly quicker payback than buying an integrated library kiosk from a commercial supplier, but this approach requires that the self check-out functions are embedded in the ILS software. This has been done in several U.S. public libraries (e.g., Fayetteville, AR). Most self check-out systems today use client software on the self check-out unit and server software on the ILS, and use the SIP or NCIP protocols.

Self check-out stations allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of books that can be stacked for simultaneous checkouts depends on the read range of the antenna. Various means have been developed to aid in the success of multiple item check-out, including anti-collision software and barriers or boxes to limit the height of items in the stack. In order to simplify the process and limit any possible errors that may affect the patron experience, some libraries allow only single item self check-out. This also provides a familiar experience for patrons who use retail self check-outs.

Self check-out stations have been tremendously successful and, while untagged items or patron circumstances—e.g., excessive fines, expired cards, address checks, and other blocks on cards—may still require a staff check-out, some libraries are seeing self check-out rates range from 30–99% of total transactions. Key factors in high rates of self check-out are intuitive, easy-to-use stations; small footprints to allow for multiple station placement; encouragement and promotion by staff; friendly loan and fines policies; and self pick-up of items on hold. Friendly fines policies may include allowing patrons to pay fines at the self check-out station using a credit card, debit account, or PayPal or increasing the threshold at which self check-out use is blocked due to fines.

1.4 Check-In, Including Manual, Conveyor, and Sorting Systems

Whether check-in takes place manually or via an automated process, RFID significantly streamlines the check-in of returned items and reduces staff repetitive motions.

Conveyor and sorting systems are becoming more prevalent in libraries with the advent of RFID technology. That's because they are less expensive and more reliable than conveyor systems that rely on barcode technology and thus require precise positioning of the materials for check-in.

The RFID reader is either mounted in a return chute or over/under a section of a conveyor belt. The item only has to pass over or under an RFID reader for less than a second—long enough to read the content on the tag, turn on the security, and communicate with the library's ILS. The item is then sorted into bins or onto shelving carts according to item type, location code, or other information. This is particularly valuable, as items on hold can be sorted into specified bins. Systems typically have anywhere from three to fifteen bins or carts, though the capability exists for a much larger number of bins. It should be understood that RFID return chutes without sorting capability will require manual intervention to perform accurately, sort for holds, etc.

Manual check-ins are made significantly easier, faster, and more ergonomically friendly with RFID, because fewer fine motor movements are required to place an item on a reader than to read the barcode with a scanner. For those using multi-item processing, more books can be checked in at one time.

1.5 Inventory Systems

RFID technology makes such mundane tasks as shelf reading, inventory control, and item location considerably faster. Early RFID-based inventory systems were limited in the reliability of their high-speed scanning of shelved items. Newer systems with faster reading protocols allow for improved accuracy.

Typical hardware offered by vendors includes an inventory wand and reader module attached to a battery-powered computer with wireless capabilities. Items on a shelf can be inventoried by moving the handheld wand along book spines.

Challenges to reliability include thin items; items in direct contact with metal shelf dividers; covers or pages with metallic ink or foil content; multiple adjacent items with tags placed in the same location; and all media items with metal content, e.g., CDs and DVDs.

1.6 Support for Interlibrary Loan (ILL)

While RFID is not necessary for ILL, it could be a powerful force for efficiency. For libraries with ILL modules built into their ILS, RFID holds the promise of streamlining staff operations. A key requirement for interlibrary use is compliance with a national or internationally accepted data model. Once a compliant environment is achieved, the receiving library staff can quickly read the unique identifier on the tag and attach it to the bibliographic record received from their bibliographic network (e.g., OCLC). This would signal that the item is received and would allow automated procedures to occur, from patron notification to self pick-up and self check-out. The borrowing institutions should not inappropriately alter any data placed on the tag by the lending institution.

Current use of RFID in some ILL processes includes being able to easily circulate ILL items by temporarily affixing a programmed tag to the item once it arrives at the borrowing institution. This not only enables self check-out but also self pick-up of holds.

1.7 RFID Standards in Libraries

There are two International Organization for Standards (ISO) standards pertinent to library RFID tags and readers: ISO/IEC 15693 and ISO/IEC 18000-3 Mode 1. ISO/IEC 15693 is the responsibility of JTC1 (Joint Technical Committee on Information Technology), SC17 (Subcommittee 17, which is responsible for developing standards for cards and personal identification). All the ISO/IEC 18000 series standards are the responsibility of JTC1, SC31 (responsible for automatic identification and data capture techniques), WG4 (Working Group 4, which deals with RFID for item management). The two standards, though related, are not equivalent. ISO 18000-3 Mode 1 has additional features and some of the features that are optional now are likely to be upgraded to requirements. The rules for AFI (discussed later in the report) are fundamentally different. Although the same silicon platform is used, the library community as it moves forward with standardization needs to ensure that the tags it uses have the required features. Having said all this, the chip and tag vendors might still refer to an

ISO 15693 tag as being acceptable for library applications. They may very well be right—the only real test is a check on the supported features.

These two standards define the wireless interface and communication protocols between RFID tags and readers. Libraries have broadly adopted the ISO/IEC 18000-3 Mode 1, standard. Further details on RFID standardization are contained in Appendix A.

Additionally, ISO JTC1/SC31/WG4 is also responsible for ISO/IEC 15961 and 15962. ISO/IEC 15961, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: Application interface*, deals with the commands and responses between the application and encoder. ISO/IEC 15962, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: Data encoding rules and logical memory functions*, deals with the process of converting printable characters or those that appear on a screen into a compacted form for encoding on the RFID tag. The encoding rules also provide a way of distinguishing between data elements using object identifiers and, particularly, the Relative-OID as discussed in Section 2.6.

Additional information on these standards can be found in Appendix E.

Section 2: NISO Data Model

2.1 Introduction

The intent of this section is to outline a data model that should satisfy the needs of libraries in the U.S. The main goal of the model is to provide interoperability for libraries so that libraries can invest in RFID with confidence that they will be able to read tags on items from many other libraries, and so that they will have choices in purchasing RFID equipment and tags in the future.

The goal of interoperability is achieved by following standards and by making sure that the data on the tag is in a standardized format and is used consistently by all users. The specification contained in the data model provides flexibility for some feature differentiation among the vendors by allowing for optional data, and by not specifying controls on how the data can be used. It also provides a minimum set of the data objects, which must be provided to perform the most basic of library functions using RFID equipment. The ultimate intention is that RFID tags programmed by one vendor in compliance with the data model will be usable by another RFID vendor without any reprogramming.

There are several data models in use in different parts of the world, including those created by groups in the Netherlands, Denmark, United Kingdom, and Australia. Most countries have adopted models similar to the Danish model (see http://www.en.ds.dk/3196) with some important variations. The approach taken by NISO is to base its work on background from these data models already in use. The NISO RFID Working Group felt that the Australian model (see http://www.sybis.com.au/Sybis/4n597-599%20proposal%20document.pdf) came closest to meeting its needs and used it as a starting point of its deliberations. It is the intent of the NISO data model to be compatible with methodologies prescribed in ISO/IEC 15961 and 15962, and to anticipate an ISO standard for RFID in libraries based on ISO/IEC 15962 (See Appendix E, Section E.1 for details). The Working Group feels that this will allow for an efficient overall system design.

2.2 Data Objects

When discussing the possibilities for recording data on RFID tags, it is important to consider that, while the *variety* of data that might be written on a tag is virtually unlimited, the *amount* of data is rather restricted. First, there is the capacity of the tag itself, which is not under the control of the library but rather is determined by the silicon and tag manufacturers. Second, there is the utility of the information on the tag; that is, how the data will be used and what value will it bring to the application. Third, it is important to keep the read time of the tag as small as possible. In some cases, more than one read may be required to retrieve all the necessary data from the tag. All of these in some way limit the amount of data that should be stored on the tag.

Broadly speaking, there are two general options for the data on the RFID tags. The minimalist approach is one safe option. In this option one would simply choose to place the Unique Item Identifier (such as a barcode) and disallow most everything else. All data required to support system functionality would have to be looked up in an associated database, such as a library's ILS. For obvious reasons, this approach is most attractive to privacy advocates. At the other extreme are those that would put as much data on the tag as space and cost considerations

would allow. The goal of this second approach is to allow the system to function with minimum interaction with the ILS. The recommendations of our data model do not exclude either approach.

2.2.1 Advantages of Looking Up Data in the ILS

Generally speaking, storing duplicate information on both the tag and in the ILS is a questionable practice as it creates a data maintenance and consistency issue. Data, particularly data that changes frequently, must be synchronized and updated in two places. Additionally, data on the tag brings us to the cumbersome requirement to have the physical item in hand to make an update. So we caution against this practice, and yet sometimes there are good reasons for doing so.

When there is a choice between storing data on the tag or in the ILS, one advantage of storing it in the ILS is the speed of accessing that data, which may be higher than the speed of reading the data from the tag.

Another advantage of storing the data in the ILS is the tag memory requirement. Database storage is relatively inexpensive compared to the memory on RFID tags, and by keeping the size of data on the tags relatively small, it allows manufacturers the possibility of producing tags with lower memory, thereby reducing the tag costs.

2.2.2 Advantages of Storing Data on the Tag

One of the advantages of storing data on the tag is in situations where, because of design or because of system failure, there is no connectivity to an ILS, or when that connection is lost for a period of time. An example of this might be the storage of a status of “non-circulating” on tags on reference materials, so that during an ILS outage the material would not circulate on a self check-out station.

Another advantage of storing data on the tag is to provide functionality that might not be directly supported by an ILS. Particular designed features of RFID systems may, in the future, require data that is not readily available from the ILS, and this data could be placed on the tag. The data model allows for this usage by defining two data objects, Local Data –1 and Local Data –2 (see Sections 2.5.14 and 2.5.15).

As a general rule, then, there are three categories of data that may be stored on the tag:

1) The minimum amount of data to support the RFID system. In the data model below, this category is in the mandatory set of data.
2) Data on the tag that enhance the operation—for example, data from suppliers that can assist with receiving functions, or data that the item is part of a set and that other items are necessary to complete the transaction.
3) Back-up data that allows the RFID system to function independently of the ILS.

All three categories are considered in the recommended model below.

2.3 Mandatory and Optional Data Objects

There is reasonable consensus in the NISO RFID Working Group that the data model should have some data objects that are mandatory and others that are optional. Such an approach has the potential of specifying a rather large tag, unless the mandatory set is kept relatively small, and the optional set are truly optional. The Working Group shied away from being too

prescriptive in its recommendations. Any prescriptive standard for the data model was seen to potentially limit development and therefore would, very likely, thwart future innovations.

Mandatory elements are those that are truly required to either make an RFID system function or to enable interoperability. These elements must be encoded on every tag, and systems can be designed counting on their presence.

Optional elements are those which may provide extended functionality or which may provide alternative sources for information that is already in the ILS. Optional elements should be supplemental data, in that the most basic functions of library operation can be performed without use of this data. In any case, the total amount of data is limited by the memory capacity of the tag over which the library industry has little or no control.

The Working Group's recommendations for each data object's designation as mandatory or optional appear in the Data Model table, below, in the column labeled "Category".

The NISO RFID Working Group felt that if there were any possibility that a data object would be used in the foreseeable future it should be included in the model and assigned a relative OID (object identifier). This would promote consistency of use across the industry. It is also the expectation of the Working Group that most implementations in the U.S. would simply use the two mandatory data objects specified below.

2.4 Locked vs. Unlocked

Most modern tags with read and write capability also offer the ability to write data into the tag and then to protect that data against further modification. This capability is typically called "locking", and is generally non-reversible. There are also tags that provide an additional feature that allow locks to be password controlled so that equipment with the password can unlock them, rendering the lock not permanent. Some tags offer this feature as a part of an accepted standard, while others offer it as a proprietary add-on feature. This data model makes recommendations on whether different data objects should be locked or unlocked.

2.5 Data Model

Table 1 describes the elements of the RFID Data Model. When the element is of fixed length, then the length is specified. If the element is of variable length and if the maximum length is known, then the maximum length is specified. However, if the maximum length is not known, then an expected length is specified, which may be much smaller than the actual maximum length.

The model specifies a total of 18 data objects. Most of the elements are variable length. It is possible that additional data objects may be added later without compromising the integrity of the model and without rendering any applications obsolete.

Table 1: RFID Data Model

Data Object	Suggested Relative OID (Likely to Change)	Length	Category	Main Purpose or Codes Used	Locked If Used?
Primary Item ID (unique item identifier)	01	Variable Expected: 16 bytes	Mandatory	Item Identification	Yes
Tag Content Key	02	Variable	Mandatory*	Determining what other data is on the tag	No
Owner Library/Institution	03	Variable Max: 16 bytes	Optional (1)	Use ISIL code (ISO 15511)	Optional
Set Info (number of parts; ordinal part number)	04	Variable 1 or 2 bytes	Optional (2)	Item Properties	Yes
Media Format	05	Fixed 1 byte	Optional (3)	Item Properties	Yes
Type of Usage: Circulating? Reference?	06	Fixed 1 byte	Optional (4)	Item Usage	No
Shelf Location	07	Variable Expected: 16 bytes	Optional (5)	Support Inventory– (LC Call Number, Dewey)	No
ILL Borrowing Institution	08	Variable Max: 16 bytes	Optional (6)	Support ILL – Use ISIL code (ISO 15511)	No
ILL Transaction ID	09	Variable Expected: 9 digits	Optional (7)	Transaction tracking	No
GS1-13 (including ISBN)	10	Variable Expected: 13 digits	Optional (8)	Identification	No
Title	11	Variable Expected: 32 bytes	Optional (9)	Identification	No
Supply Chain Stage	12	Fixed 1 Byte	Optional (10)	For multi use	No
Supplier Item ID (Alternate Item ID)	13	Variable Expected: 16 bytes	Optional (11)	Acquisitions Supply Chain	No
Local Data –1	14	Variable Expected: 10 bytes	Optional (12)	Internal data	No/Yes
Local Data –2	15	Variable Expected: 10 bytes	Optional (13)	Internal data	No/Yes
Order Number	16	Variable Expected: 12 bytes	Optional (14)	Acquisitions	No
Invoice Number	17	Variable Expected 16 Bytes	Optional (15)	Acquisitions	No
Supplier Identification Data	18	Variable Expected 32 bytes	Optional (16)	Acquisitions	No

*See Section 2.5.2.

2.5.1 Primary Item ID

The Primary Item ID is the identifier that is used to uniquely identify an item within a particular library. Most typically this is the barcode on the item and is the identifier used in functions like circulation (both check-in and check-out) and inventory management. (Note: Please see Section 2.5.12 on supply chain stage as it impacts Primary Item ID.)

Properties:

a) Mandatory

b) Variable length supporting full ASCII character set (expected length 16 bytes)

c) Locked (when used in library; unlocked in supply chain)

2.5.2 Tag Content Key (also called OID Index)

The second mandatory data object is the tag content key. The tag content key is designed to allow RFID applications to determine very quickly what data, if any (other than the Primary Item ID), exists on the tag.

The content key is essentially a binary flag indicating data objects, starting at relative OID 3, that are present on the tag. Since the model has a total of 18 data objects and two of them are mandatory, then only 16 bits are needed to flag the 16 optional data objects. It is necessary to maintain byte boundaries in encoding the data. Since there are exactly 16 optional data objects only two bytes are needed. An example follows:

> In addition to the two mandatory data objects, assume that the tag has two optional elements encoded on it. Further assume that the two elements are owner library and ISBN. According to the model, these are the first and the 8th optional elements. Thus, the content key will be coded with 1 in the first and 8th position and zeroes elsewhere. The encoding therefore will be
>
> Code: 1000000100000000
>
> Position: 1234567890123456
> (showing 16 bits in use)

If only the mandatory fields are on the tag, then the code string will have all zeroes. An all zero string will tell the application that there is no other data on the tag. There is one other very important implementation option presented below.

The mandatory nature of this data object is linked to the presence of optional data items on the tag. If there is other data on the tag, then this data object is indeed mandatory. However, if there is no other data on the tag, then this data object can either be included with its content as all zeroes or it can be omitted altogether. The absence of this data object from the tag implies, with certainty, that there is no other data on the tag. This particular implementation has the great advantage that all existing ISO/IEC tags with only the Primary Item ID on the tag can be made to interoperate with newer systems by automatic software conversion when the tag is read. Essentially, the software will have to recognize that the tag is not a compliant tag and then reformat it to a compliant coding scheme described in this document. This will facilitate interoperability with existing tags, requiring only minor software changes at the reading station.

Properties:

a) Conditional – It is mandatory if another optional category data element is encoded.

b) Variable length – dependent on the encoded data set on the tag.

c) Unlocked

2.5.3 Owner Library/Institution

This element is used to identify the owning library. This identification is useful in ILL functions and in material flows in consortium networks where patrons are allowed to return borrowed books to any library in the consortium.

It is suggested that the ISIL code be used for this data object. According to the Registration Authority for ISIL (ISO 15511): [2]

> The ISIL is a variable length identifier. The ISIL consists of a maximum of 16 characters, using digits (Arabic numerals 0 to 9), unmodified letters from the basic Latin alphabet and the special marks solidus (/), hyphen-minus (-) and colon (:). Each ISIL identifier shall be unique. When an ISIL is written, printed, or otherwise visually presented, it shall be preceded by the letters ISIL separated from the identifier by a space. An ISIL is made up by two TC46 SC4 N552 components: a prefix and a library identifier, in that order, separated by a hyphen-minus. The hyphen-minus is a mandatory character in the ISIL string.
>
> A country code identifies the country in which the library or related organization is located at the time the ISIL is assigned. The country code shall consist of two uppercase letters in accordance with the codes specified in ISO 3166-1.
>
> A non-country code prefix is any combination of Latin alphabet characters (upper or lower case) or digits (but not special marks). The prefix may be one, three, or four characters in length. The prefix is registered at a global level with the ISIL Registration Authority.
>
> Library identifiers are defined by the national Registration Agency or a non-country agency and are unique worldwide. The Library identifier will have up to 11 character positions without blanks between country code and national identifier.
>
> The Registration Authority has establish [sic] the website http://www.bs.dk/isil and information about national Agencies are updated here.

Properties:

a) Optional

b) Variable length not to exceed 16 bytes with formatting as specified above

c) Locked if used

2.5.4 Set Information (also called “multi-part indicator”)

This data element is useful if several components (like a book and a map, a board game and a manual, or if multi-part, multimedia components are circulated as a single unit).

[2] ISO 15511 (ISIL) Registration Authority, *Report of the ISIL Registration Authority,* TC46/SC4 N552, (October 12, 2004). http://www.niso.org/international/SC4/n552.pdf

There may be a single RFID tag on the items that are circulating or each separate item may have a tag of its own.

The set information is presented in two components: The ordinal part number followed by the total number of parts. If the total number of parts is nine or less, then the user data can be presented as a 2-digit code. If the total number of parts is between 10 and 99, then the user data is presented as a 4-digit code. (See Section E.3 in Appendix E.)

Properties:

a) Optional (but recommended for multi-part items)

b) Variable length of one or two bytes

c) Locked if used

2.5.5 Media Format

This data object is used to specify the format of the media being circulated. Several codes are available to describe this element.

The NCIP standard, ANSI/NISO Z39.83, Part 2, identifies several media types, but does not designate a code for them. The Danish RFID data model does describe a coding scheme that consists of 256 codes and therefore can be encoded in a single byte. At this point, it is the inclination of the NISO RFID Working Group to adopt the ONIX Encoding Scheme for media format, which is widely supported by BISG (Book Industry Study Group) in the United States.

A list of possible code values is provided in the Appendix D.

Properties:

a) Optional

b) Fixed length of 1 byte

c) Locked if used

2.5.6 Type of Usage

This data object provides information about the intended use of the item. For circulation purposes, the value of interest is whether the item is allowed to circulate or not. A full table of values is being considered and may be helpful in locating misplaced and lost items.

Properties:

a) Optional

b) Fixed length of 1 byte

c) Unlocked

2.5.7 Shelf Location

In the U.S., there are three primary methods of shelving books. These are:

- By Library of Congress (LC) call number
- By Dewey Decimal classification
- By type of material (like FIC for fiction), concatenated with some characters of the Author's Name. This method is used primarily in public libraries.

The LC call number is usually taken from Library of Congress Classification or from the LC Classification Additions and Changes. In the MARC 21 format, it generally includes subfields a and b ($a and $b).

The Dewey Decimal Classification number is usually taken from Dewey Decimal Classification, Abridged Dewey Decimal Classification, and/or DC&: Dewey Decimal Classification Additions, Notes and Decisions.

The purpose of this data object is to allow a library to choose its shelving method and specify it here. Automatic sorting systems sometimes use derived code, like a collection code, which is pulled from the ILS and used for sorting purposes. It could also be used in shelf-reading or inventory applications by a scanner in the library stacks area.

Alternatively, this field could be used for specifying exactly where the book is to be shelved—for instance, 3rd floor, shelf 14. This latter method of designation is not recommended, as a change in shelving location will require the handling and reprogramming of the tag.

Since this data object is to be used within the library, it is not necessary to identify whether the data object is an LC call number or a Dewey Decimal number or a number from some local numbering system. The classification system information could be configured into the system setup rather than obtained from the tag.

Properties:

a) Optional

b) Variable length

c) Unlocked if used

2.5.8 ILL Borrowing Institution

This element is used to identify the borrowing institution in an ILL transaction.

The coding scheme should be identical to the owner institution described in Section 2.5.3, except that this data object is always unlocked.

Properties:

a) Optional

b) Variable length not to exceed 16 bytes with formatting, as specified in 2.5.3 above

c) Unlocked if used

2.5.9 ILL Transaction ID

In addition to the ILL Borrowing Institution data element, there is additional data that will facilitate the tracking of ILL transactions. In interlibrary loan transactions In the U.S., the process generally has the following steps:

1) The library customer or patron identifies some material that s/he wishes to borrow, and works with library staff to arrange for an ILL search.

2) The library staff at the borrowing library use ILL management software to access a catalog of items owned by other libraries, and select some candidate lending libraries for the item. The ILL management software generates an ILL transaction identifier, often a numeric identifier of seven or eight digits. One example of an ILL

management software system is OCLC's ILLiad system, and an example catalog is OCLC's WorldCat.

3) The ILL management software initiates contact with the first candidate lending institution, requesting a loan of the item, identified bibliographically.
4) The candidate lender looks at the request and, if it is able to fill it, responds affirmatively. If it is not able to fill the request, it responds negatively and the ILL management software sends the request to the next candidate lending institution on the list.
5) When a candidate lender indicates that it can source the item, the ILL management software stores a record and generates an ILL slip containing the transaction identifier, the bibliographic identifier, the borrowing library information, the lending library information, and the patron information. The ILL slip accompanies the item as it travels from the lending library to the borrowing institution.
6) When the borrowing library receives the item, it generally creates a temporary record on its integrated library system (ILS), using a "dummy" or temporary item identifier. The library uses bibliographic information from the ILL management software to populate the record.
7) The library patron is notified and picks up the item, which is sometimes packaged in a bag or with an attached slip, but which has the dummy item identifier attached in some way.
8) At the end of the loan, the patron returns the item to the borrowing library, which notes on the temporary record that the item is returned, and sends it back to the lending library.

The one common piece of data between the borrowing library and the lending library is the ILL Transaction ID, generated by the ILL management software system. All other data regarding the ILL transaction can be obtained from the ILL slip or through management software, based on that ILL transaction identifier.

It is feasible (and desirable) that, in the future, an ILL Transaction ID could be read electronically and used to automatically update a temporary ILS record with data regarding the item and transaction, eliminating part of the manual labor associated with the transaction and reducing costs.

Properties:

a) Optional
b) Variable length – expected to be 9 digits
c) Unlocked if used

2.5.10 GS1 Identifier (includes ISBN)

The ISBN (International Standard Book Number) is assigned to a monographic publication by designated agencies in each country participating in the program. The field may include terms of availability and cancelled or invalid ISBNs. In the MARC21 format for bibliographic records, this data is contained in 020 tag subfield a ($a).

ISBN applies only to books. CDs and other media format use an identifier called GS1 Code.

The GS1 Code is more popularly understood in the United States as the UCC Code, and commonly seen in retail outlets in a bar code format. *This includes the encoding of the ISBN, with the prefix '978', and more recently '979'*. Since January 2007, the ISBN has formally changed from being a 10-digit code (sometimes with an X check character) into a 13-digit code, as represented in the GS1-13 barcode.

The GS1 code is applied to various other media products, including CDs, DVDs, and some periodical publications and music. There is a scheme for linking the ISSN (International Standard Serial Number) for serial publications to the GS1 code with the prefix '977'. There is also a scheme that links the ISMN (International Standard Music Number) for printed music to the GS1 code with the prefix '979', shared with the ISBN.

The code structure for CDs, DVDs, and other products without formal registration code structures follow conventional GS1 rules. This means that for many products that originate in the U.S. the code might need to be expanded with leading zeros to conform to the 13-digit structure. Codes on products from most other countries use the full 13-digit structure. Encoding everything in a 13-digit structure is important because the final digit is a check digit that may be used for validation processes in some systems (see Section E.3.5 of Appendix E).

Properties:

a) Optional

b) Variable length – expected to be 13 digits

c) Unlocked if used

2.5.11 Title

This element is the title of the library object.

Properties:

a) Optional

b) Variable length – no maximum length specified, though the expected length is 32 bytes

c) Unlocked if used

2.5.12 Supply Chain Stage

As explained in Section 5, the NISO RFID Working Group worked under the hope that RFID tags would eventually be placed on the books during the manufacturing process prior to library distribution, and therefore has endeavored to make the data model adaptable enough to function throughout the supply chain, should that become a reality. As an example, it is conceivable that an RFID tag would be placed on a book by its manufacturer, then used by the publisher, followed by the book jobber, and finally by the library. We hasten to point out that, at least in the U.S., there is no coordinated effort to make this happen. At this point it is only a hope. Though some members of the Working Group have embraced this cause in earnest and are taking steps to discuss this possibility with upstream members of the supply chain, the standards that we are participating in are, at the moment, only applicable to libraries. Even the international effort to synchronize the data model across nations goes under the title: *Information and documentation – Data model for use of radio frequency identifier (RFID) in libraries* (ISO/NP 28560).

At this point, the requirements of other parties in the supply chain are not known. Different uses of the tag at different points in the supply chain or the lifecycle of the tag would require different data objects to be stored on the tag. Our focus is on the library application. Our general recommendation is that the data objects, where appropriate, be left unlocked so that there is the possibility of broader use of the tag. This data model is designed in a manner that does not preclude its use in other stages of the supply chain.

To make this desire more explicit, the NISO RFID Working Group is adding a "Supply Chain Stage" data object on the tag to allow different data to exist on the same tag at different stages in the life cycle, and to make it clear to an RFID application system what data may be expected on the tag at a particular time in its life. The "stage" data object corresponds to the stages of the tag's lifecycle. At each stage, the users of that particular stage can define different optional elements to reside on the tag.

The following stages in the supply chain have been identified:

- manufacturer (use data object value = 16)
- publisher (use data object value = 24)
- distributor (use data object value = 32)
- jobber (use data object value = 48)
- library (use data object value = 64)

Initially, the NISO RFID Working Group thought that this data object should be mandatory. However, after discussions with several individuals, the Working Group decided not to include this data object as a part of the mandatory set, but rather make it optional. This decision would appease the international library communities and yet keep the door open for any communications and negotiations with other members of the U.S. supply chain.

Properties:

a) Optional

b) Fixed length of 1 byte with values shown above (other values may be added later)

c) Unlocked if used

2.5.13 Supplier Item ID (Alternate Item ID)

The Supplier Item ID (not necessarily a unique ID) is assigned by the supplier to identify the title being delivered to the library. It may or may not be the ISBN or the UPC code number. This number has application (or meaning) only to the supplier and is used to return books to the supplier.

Properties:

a) Optional

b) Variable length – alphanumeric data with expected length of 16 bytes

c) Unlocked if used

2.5.14 Local Data –1

As previously stated, the NISO RFID Working Group felt that it was important to allow some local flexibility in the data model. The local data object is designed to do just that. No

specification is provided for this object. This allows libraries to code one or more fields in a format of their choice to support functions that may be thought of in the future. There is no external application of this data object, so the library may use it exactly as it chooses.

Properties:

a) Optional
b) Variable length
c) Unlocked if used

2.5.15 Local Data –2

A second data object, similar to Local Data –1.

Properties:

a) Optional
b) Variable length
c) Unlocked if used

2.5.16 Order Number

This data object contains the library's order number against which the item was purchased.

Properties:

a) Optional
b) Variable length – alphanumeric data with expected length of 12 bytes
c) Unlocked if used

2.5.17 Invoice Number

This data object contains the supplier's invoice number against which the item was paid.

Properties:

a) Optional
b) Variable length – alphanumeric data with expected length of 16 bytes
c) Unlocked if used

2.5.18 Supplier Identification Data

This data object is designed to uniquely identify the supplier of the material in question. It consists of a supplier name, address, and postal code (or SAN). The exact coding of this is still under discussion.

Properties:

a) Optional
b) Variable length
c) Unlocked if used

2.6 Relative OID

Each data object on the tag has a unique identifier (UID). Instead of using the entire identifier, it is more economical to use the relative object identifier (OID). The NISO RFID Working Group found a good explanation of relative OIDs in the work done by the Standards Australia Working Group. Their explanation is being reproduced below with permission. The original explanation may be found on pages 10-11 of the Standards Australia Working Group IT-019-01-02 *Proposal for a Library RFID Data Model* (September 2006) document (http://www.sybis.com.au/Sybis/4n597-599%20proposal%20document.pdf) that describes relative OID and includes a rationale for the 14 elements on the OID:

> 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.

2.7 Encoding

Discussions of data models naturally turn to encoding fairly quickly. One of the benefits of the ISO/IEC 15962 specification is that it allows the discussion of data objects to move up a level of abstraction above the point where encoding is important. ISO/IEC 15962 specifies methods for compacting different types of data efficiently into objects for storage in tag memory, and then for expanding that data back out of the tag and into formats useful at the application level.

For example, say one library uses a 14-digit numeric barcode as the item identifier, as many libraries do in the U.S. ISO/IEC 15692 suggests that this might be recognized as an integer and stored efficiently on the tag using between 3 and 4 bits per digit (up to around 50 bits for a 14-digit integer, encoded in 7 bytes). Imagine another library using a 12-character alphanumeric item identifier using digits 0-9 and characters A-Z. In this case, the identifier can be characterized as uppercase/numeric and stored efficiently on the tag using 6 bits per character for a total of 72 bits (9 bytes). In each case, there is some object definition overhead that is also stored on the tag to identify the data objects and to tell how they are stored.

The important part of this is that it allows different libraries to correctly interpret tag data that is efficiently encoded without applying a rigid standard on exactly how the encoding is to be done. ISO/IEC 15962 allows encoding of numeric, alphanumeric, ASCII, and UTF-8, which should

cover most all encoding requirements for U.S. libraries. The corresponding fields on different tags might even be encoded differently within the same library based on individual item characteristics, resulting again in the most efficient encoding while maintaining a good system design.

Appendix E shows details on the encoding scheme being proposed by the ISO committee.

2.8 Use of Primary IDs and Supply Chain Stages

As previously stated, the level of interoperability anticipated in this model would permit the same RFID tags to be employed at any point in the supply chain—whether embedded at manufacture of the item, applied in distribution, or used by the jobber. The advantages of this interoperability have been described in Section 5, and while the data model proposed should work for all uses, there is a caution related to the unique item identifier (UII) that must be specifically addressed.

At whatever stage in the supply chain RFID is applied for item-level processing, the UII is a mandatory and critical data object. But it is important to note that, even if it is imagined that the same tags could be applied at any stage of use, it is not to be expected that the same identifier will be employed at every stage as items transfer from one stage of the supply chain to the next. For example, a book distributor may track inventory via item-level RFID using EPC codes as Primary Item IDs. A jobber may then receive from this distributor tagged books that the jobber must then process for the library use—processing that includes recording library-specified data to the RFID tags.

In order for item-level RFID tags to be usable throughout the supply chain, including in retail or library operations, the NISO RFID Working Group recommends the following:

- Primary Item ID must always be mandatory. However, the supply chain stage must also be encoded. This data is essential for the RFID applications to work correctly.
- Primary Item ID data object in other stages of the supply chain must be left *unlocked*. This will allow users further along the supply chain to apply their own identifiers, whereas if this field is locked only those users sharing the database to which the IDs are associated can make use of the tags. It is also thought that concerns about vandalism—deliberate alteration or removal of identifiers on tags—are of far less concern at the earlier stages of the supply chain, where items are less exposed to the public. Concerns about accidental alteration or removal of IDs can be addressed by the use of UIDs to back up tag data. If this precautionary approach is followed, in the library stage the link between the UID and Primary Item ID is mandatory. However, in earlier stages it is not essential, so in those stages the UID may act as the only identifier.
- Primary Item ID data object in “library” stage should be *locked*. In library settings where items are made accessible to the public, the Primary Item ID field should be locked as an additional precaution against vandalism or accidental alteration or erasure.
- All optional data objects in upstream use stages should be left unlocked. As with Primary Item ID, the data recorded on the tag at one use stage may not be required or desired at subsequent stages.
- Due to privacy concerns and to reduce the size of the tags required, it is recommended that tags that might have originated in an earlier stage of the supply chain be reprogrammed for use in libraries. For example, an ISBN that might be

useful earlier in the supply chain becomes a privacy issue if it remains on a library tag. Therefore, these tags should be blanked out by the library or jobber and reprogrammed with contents the library needs and wants, in accordance with the model.

2.9 Comparison Between NISO Data Model and Australian Data Model

A comparison of the NISO data model with that of the Australian proposal is provided in Appendix C of this document.

Section 3: Security

3.1 RFID Security for Libraries

There are several approaches available for securing library items using RFID, each with its own advantages and drawbacks. These approaches include dedicated electronic article surveillance (EAS) implementations, application family identifier (AFI) byte implementations, and virtual deactivation (database look-up) implementations.

Each of these security methods has different characteristics for speed of detection, reliability of detection, and susceptibility to tampering.

A great number of variables affect the characteristics of all RFID security systems, including:

- width between security gates,
- number of items simultaneously exiting the library,
- material of which the items are made,
- size of the RFID tags,
- tuning of the antennas on the RFID tags,
- orientation of the tags in the portal,
- tags' relative positions to each other, and
- whether the system time-multiplexes multiple security methods.

The characteristics of different systems in terms of speed, reliability, and security are part of the manufacturer specifications, with standards focusing on interoperability. It is important for any RFID standard for libraries to focus on the key requirements for interoperability while allowing for differences between solutions that foster healthy competition in the marketplace, and to allow for the development of more advanced solutions as technology evolves.

The following sections describe three methods of security for library items using RFID.

3.2 AFI

Application Family Identifier (AFI) is a hardware feature designed into the silicon chip on ISO/IEC 18000-3 Mode 1 RFID tags. The purpose of AFI is to prevent tags from different industry applications from interfering with each other in the open environment. AFI is a special purpose register in a dedicated portion of the memory of an RFID tag. The register is 8 bits in length and two hexadecimal symbols can be used to describe the bit pattern. The hardware design of the tag allows modifying the behavior of a tag by programming this register. Specifically, the programming of an ISO/IEC 18000-3 Mode 1 compliant tag with a particular AFI code dictates that the tag will respond only when an interrogating reader system requests a response from tags with that AFI code. This facilitates both security implementations and separation of applications.

Security implementations based on AFI require that a particular code be programmed in the AFI register of tags on library items that are checked into the collection. The portal at the library exit

interrogates its surroundings for any tags with that AFI code. Tags with this code in the AFI register respond with their unique identifier, and tags with other codes in their AFI registers do not respond.

The following subsections outline the fundamental elements required to facilitate interoperability, while allowing for multiple security methods for RFID in the library industry.

3.2.1 AFI Codes and Interoperability

To facilitate real interoperability, all libraries should be utilizing standardized tag protocols. ISO/IEC 18000-3 Mode 1 is the standard most widely used in libraries at this point, and this standard supports AFI.

To further facilitate interoperability, all library RFID systems, regardless of security method, should use AFI codes authorized by ISO for use by libraries for library items. This facilitates interoperability with other applications. Such codes were requested in 2005 by U.K.-based EDItEUR, and supported by information on AFI use in libraries provided by NISO.

On September 11, 2006, ISO JTC1/SC31/WG4/SG1 discussed and identified two codes that can and should be used for library RFID applications using AFI for security. One of these codes $(C2)_{HEX}$ is the official assignment for the library industry and should be used on items that are checked out and circulating in the open environment, whether or not AFI is used for security. The use of this code will provide for application separation so that library materials do not interfere with other non-library applications. The other code $(07)_{HEX}$ is slated to be included in a redrafted version of ISO/IEC 15691 Part 3. It is one of the several codes controlled by SG1 which can be used for closed applications, and this is the code which should be used on library items that are checked into the library and that are being secured by systems utilizing AFI for security.

Systems that use AFI for security should use both of the assigned codes as appropriate, while systems using EAS or database look-up for security should use the library industry code to avoid interference with other applications of RFID.

3.2.2 AFI Locking

Locking is a hardware feature available on most ISO RFID tags that allows a tag programmer to make the contents of a portion of a tag's memory permanent so that it cannot be modified. In some designs the lock may be reversed using a password, while in other cases, permanent really means permanent. In general, locking protects against accidental or malicious modification of tag contents.

All library RFID systems should utilize design practices that do not limit the library's options for the future. Specifically, AFI codes on tags for use in library items, even when programmed by systems that do not utilize AFI for security, should be left unlocked, allowing for later modification should the library wish to use AFI for security in the future.

3.2.3 Interlibrary Loan Situations

Interlibrary loan, for this discussion, refers to the borrowing of library items that belong to another library system. It does not refer to inter-branch borrowing within a multi-branch library system.

Systems should be designed so that should an AFI code or EAS bit be changed during an interlibrary loan event; they will seamlessly reprogram the AFI code or EAS bit on the item back

to the original setting upon its return to the owning library. The burden for this reprogramming lies on the system that checks the item back in to the owning library.

3.3 Electronic Article Surveillance (EAS)

Traditional electronic article surveillance (EAS) architectures, as seen in many retail applications, are based on radio frequency (RF) tags rather than RFID tags. These systems employ a tag that resonates when excited by an exit gate. The resonance can then be sensed by the gate, which in turn generates an alarm.

The EAS concept has been introduced to some RFID tags. A difference, however, is that rather than a single resonance, the tag responds with a short burst signal or short data transmission.

This kind of EAS technology is built into some, but not all, ISO/IEC 18000-3 Mode 1 compliant tag designs as a proprietary add-on feature. This technology typically provides a tag with a one-bit register, programmable on or off, which determines the tag's response to an EAS command from an interrogator, or in some cases just the presence of the security gates. If the bit is turned off, then the tag does not respond to an EAS command from the interrogator, and if the bit is turned on it does respond to such a command. If the portal interrogator detects an EAS response from a tag, it generates an alarm.

EAS security methods do have some benefits over AFI implementations, in some cases offering longer detection range, higher speed of detection, and increased protection against tampering.

As mentioned earlier, EAS implementations are typically proprietary. As such, it is likely that detection systems using EAS detection methods, designed for use with RFID tag silicon from one manufacturer, will not provide security on items with tags from a different silicon manufacturer. Nonetheless, by adhering to the interoperability guidelines in Section 2, the system designer can ensure interoperability for identification and non-interference in other library RFID implementations.

3.4 Virtual Deactivation (Database Look-Up)

The virtual deactivation, or database look-up, method consists of reading an ISO tag's unique identifier and looking up the security status of that item in a database table. The method is not limited to ISO tags, but is applied to ISO tags in the context of the Working Group's goals for interoperability.

Essentially, database look-up systems maintain a database of the identifiers of items that are checked in or out of the library. They employ techniques that interrogate their surroundings for any relevant tags, read the identifiers from those tags, and look them up on the database to determine the items' check-out status. These systems then generate an alarm when they determine that an item that is not checked out has passed through the detection system.

Database look-up is generally based on reading the ISO tag unique identifier (UID). This is the 64-bit unique identifier programmed in all ISO/IEC 18000-3 Mode 1 Integrated Circuits (ICs), by the IC manufacturers.

The UID is programmed by an IC manufacturer and doesn't require tag programming for the security feature. The only requirement is for the ISO tag reader to capture the UID (which it already does as a part of its normal processing) and pass it to the security system, which then determines the security status of the tag, which is stored in a database look-up table.

3.5 Recommendations for Security

By accepting the simple guidelines outlined below, a library purchasing a compliant RFID system from any vendor should have an interoperable system to the following extent:

- The system will cause no interference with other applications.
- The system will utilize ISO/IEC 18000-3 Mode 1 tags programmed so that they should work for identification of items in other libraries.
- The system will use tags that can be used for security in some but not all other libraries.
- The system will use tags that will not interfere with the operation of security systems in other libraries.

Refer to the table in Appendix B for an additional summary of interoperability characteristics.

AFI would appear to be the best choice for implementing a standard security solution for the library family of applications for the following reasons.

- It is already a mandatory part of the ISO standards—all ISO/IEC 18000-3 Mode 1 compliant tags and readers must support this command.
- It allows libraries to purchase systems from different vendors, still permitting them to share materials through interlibrary loan and providing security for the item in the borrowing library.
- It allows a library to purchase tags from different ISO-compliant tag suppliers.
- It provides an efficient process for security.
- It can be implemented and still allow for other security methods.
- It provides a filter, such that all library systems will only process tags that belong to the family of library applications.

AFI enables systems that use different methods to process security information to coexist and facilitates interoperability, vendor differentiation, and competition.

Systems that feature different security methods are able to operate in AFI based systems. This is an aspect of the AFI element being a mandatory part of the ISO/IEC 18000-3 Mode 1 standard. It enables the AFI method of security to be used in AFI based systems, regardless of the chosen security method for a particular system. Refer to Appendix B for interoperability characteristics.

This Working Group recommends an approach to standardization in security for RFID in Libraries that does not lock a compliant system into any single one of the possibilities outlined, but promotes security as a place for differentiation between vendors.

This can be done in a way which provides interoperability and which does not force reliance on any particular proprietary security architecture. The NISO RFID Working Group further recommends that the guidelines for interoperability outlined in Section 2 be adopted to ensure that interoperability of item identification between systems is maintained. Please note that:

- An ISO library system's security function can interoperate with any other ISO system by specifying a standard implementation for security using the AFI byte.

- The AFI byte should be standardized to define a tag as belonging to the family called "library applications."
- The AFI byte should be selected for standardizing security, because it is a mandatory ISO command and all ISO readers must support the command to be compliant.

It should be noted that, as indicated in Appendix B, it is not possible, under this recommendation, to provide interoperability of security between systems in every case.

Section 4: Migration to ISO Standard Tags

4.1 Introduction

Some librarians are concerned that today's tags and system components may become obsolete, thereby requiring expensive and time-consuming retagging operations. This can be avoided to a great extent by purchasing tags compliant with: (1) ISO/IEC 18000-3 Mode 1 (air interface), and (2) the data model recommended in this document. However, while the prospect of migrating from proprietary to standardized systems can be daunting, with some careful planning and a good understanding of an organization's goals, the labor and disruption involved can be minimized.

Many libraries over the past several years have purchased tags conforming to ISO standards with the hope that this would make the tags interoperable with systems in use in other libraries. There are several complications to this issue, one of which is the main purpose of RFID standardization activities in the library industry today—there is no existing standardized data model for the storage of data on library RFID tags in the U.S. or across most of the world. While ISO-standard RFID tags conforming to ISO/IEC 18000-3 Mode 1 are compatible with multiple vendor systems at the most basic hardware level, sometimes referred to as the "air interface," different vendors store the data on the tags in different ways.

Libraries that are not concerned about interoperability or have collections that are not shared may not consider migration as an important requirement. For libraries desiring migration to a standardized system, the issues are more complex.

Yet all is not lost, because most standards activities undertaken today on a global basis are suggesting that these very tags are a good choice for interoperability. If the systems used to program the tags for use in the library have been configured for a future migration, then there are strategies that a library can use to move toward standards that are adopted by the industry. Here are some important considerations to enable this migration:

- The tags should be reprogrammable. Most ISO tags are programmable many times, but if the programming system is configured to lock the contents of the tag after programming, then they are no longer programmable. Systems vendors and libraries can work together to ensure that there is a path forward for libraries by leaving systems open for forward migration.
- It is possible for RFID systems to recognize multiple tag data formats at once and to assist with the migration. It is not necessary for libraries to reconvert overnight to support a new standard, but it is prudent to ensure that equipment upgrades are made before tags are reprogrammed so that the user experience is maintained without excessive errors, etc.

Some of the pros and cons of upgrading or migrating to a standard should be recognized here. First, some of the pros:

- Interoperability between libraries: This is a primary goal of the standardization activities. Libraries want to be able to read tags that are affixed to items owned by other libraries and that in many cases were programmed by systems produced by other vendors. By upgrading systems to support standards and by migrating tag data into standard formats, we can achieve this kind of library–to-library interoperability.

- Good citizenship: The AFI on an RFID tag is a means of ensuring that the application of RFID in the library industry does not interfere with RFID uses in other areas, and vice versa. To be good electronic citizens, we should make sure that we are ISO compliant and using an officially assigned AFI code. The codes are referred to in Section 3.2.1.
- Vendor equipment replacement: This is the other aspect of interoperability. Libraries are concerned about the future value of their investments, and are resistant to the concept of being locked to a particular vendor based on past choices. By migrating tag data formats to a standard, in the future, when equipment upgrades and expansions are considered, the library may select and even mix and match components from standards-compliant system vendors. This is a benefit because it encourages competition, drives innovation, and reduces the need for compromises by the library.

And some of the cons:

- Information about tag formatting is public: Standards and data models are, by their nature, public documents. In other sections of this document we have described how a sufficiently informed or clever vandal or thief might use an RFID reader to vandalize tags or to steal an item from a library. There is a finite risk in migrating to a standard and therefore to a publicly available data format. However, this is only an incremental difference from the proprietary data formats, which, unless truly encrypted, are generally not difficult to decipher for a technically oriented individual with an RFID reader.
- Labor requirements: There will be some labor requirement for a migration to any new data model such as the one described here. There will be work involved in equipment upgrades and, where personnel are employed to reprogram tags, that will consume staff time as well. The labor required for a migration can be minimized through thoughtful planning.
- System performance: During a migration period, when systems will need to deal with two tag data formats, there will be some small but perhaps noticeable performance reductions in different pieces of equipment. For example, if a security gate must run two security protocols in alternating fashion, perhaps for a second or so (probably less) for each protocol, the overall rate of detection will be reduced.
- Upgrade costs: There is always a cost associated with changing equipment and software, and how this cost is absorbed by the industry will probably vary from vendor to vendor and library to library.

The needs of the book jobber in this discussion are more difficult to quantify, since these needs are somewhat defined by the equipment, software, and tags in use in their customer libraries. Ultimately, with or without new standards, book jobbers do their work for the libraries, and they need to meet the requirements of the libraries to maintain satisfied customers. However, tags that are standards compliant for interoperability will open up the possibility that jobbers can use the same hardware for all standards compliant tags as long as the software/firmware is programmed to handle any unique vendor system requirements.

The problems faced by book jobbers, outlined in Section 5.4, are diminished as more libraries adopt standards, allowing the book jobber to utilize a standard tag and programming scenario on higher percentages of processed materials.

4.2 User Considerations in Upgrading (Are my RFID tags upgradeable?)

Some of the RFID tags in use in libraries today are compatible with ISO standards (ISO/IEC 18000-3 Mode 1), and some are not. Specific questions about compatibility should be directed toward a library's RFID vendor. But there are some general characteristics about compatibility that we should understand.

First, it is not possible to upgrade a proprietary tag design to an ISO tag design via reprogramming. ISO tag and proprietary tag designs use different silicon chips. Proprietary tag designs generally do not include features such as the application family identifier feature, though they may include additional capabilities such as security features, password protection, etc., which are not covered by current standards.

Second, it may be possible to reprogram even a proprietary RFID tag to utilize a standardized data format, taking us one step further toward interoperability even with the proprietary silicon. The capability of different systems to deal with this situation will vary and not much can be guaranteed, so the return on such an effort may well not be worth the investment, but it does fall within the scope of possibilities.

Third, libraries that have collections with proprietary tags should not despair of being conformant to standards. One general characteristic about library collections is that they turn over, especially in public libraries, which are currently adopting RFID at higher rates. A library with an existing collection tagged with proprietary tags could decide to switch to standardized tags and formats for their future acquisitions, and over time their collection would become predominantly and perhaps completely standard compliant. A library RFID vendor should be able to provide systems that would work with both types of RFID tag and format in the same library.

4.3 Role of RFID Vendor

The library should expect that the vendor would monitor standards activity and will plan, develop, and offer market solutions that comply with the standards. It may be necessary to make hardware upgrades to equipment in the library if that equipment does not work with standardized RFID tags. It is also likely that software upgrades will be required on equipment in the library even if the library is already using standardized tags such as those specified in ISO/IEC 18000-3 Mode 1. This software will support the new way that data will be stored on tags to conform to a standard, and probably will need to support the old way of storing the data as well, at least during the migration period. Configuration changes may be required in security gates, moving from one type of security protocol to another, or, in the case of AFI for security, perhaps from one code to another.

4.4 Suggested Migration Process

There are several processes that can be used for migration. Let's think about the tags first. Most libraries will do their tag migration "on the fly" or "systematic" to varying degrees. Let's define these terms first. An on-the-fly migration of tags refers to one where the tags are reprogrammed to a standard data format during some activity that is already happening on the item, such as during a circulation operation. A systematic tag migration refers to one where the tags are reprogrammed using a deliberate process of moving through the stacks with a reprogramming device, operating on each item.

Let's first consider on-the-fly migration. There are several devices that can be used for reprogramming tags in this kind of migration, including self check-out devices, staff workstation devices, and automated check-in devices. Tag reprogramming can be done on check-out or on check-in, and can be done automatically by the equipment involved. For the least impact on perceived system performance, it is worth considering reprogramming tags during check-in operations, when the patron is less directly involved. For example, if your library system uses self service check-out, and an automated sortation system for check-in, you might consider having the self check-out station recognize both the new standard tag data format and the old proprietary format, but have the sortation system reprogram proprietary-encoded tags to meet the standard upon item return. In this way, the patron is not burdened by any errors or performance penalties that may arise were the self check-out station to attempt to reprogram the tags on a stack of items, and the sortation system can separate out any items that do not successfully reprogram for staff intervention. It may still be necessary to go out into the collection, perhaps with a handheld reader, to find infrequently circulating items that have not been reprogrammed after a time period following the start of the migration.

Next, let's consider systematic migration. In this scenario, the library would go into the stacks using a reader, which could be used at the location of the items on the shelf to reprogram the tags to the new standard format. At the same time, it would be important to quarantine any returned materials to ensure that no proprietary data format tags are introduced into recently migrated sections of the collection. These returned materials would need to be migrated before reshelving.

It is probable that the systematic migration would require more staff labor to implement, yet it is quite likely that it would take less calendar time than the on-the-fly method. Each method has drawbacks and advantages, and some of these may affect different libraries differently due to unique characteristics of the collection or the policies in place. Libraries will also need to make individual choices about particular processes. For instance, a library that does a lot of interlibrary loan will probably want to consider reprogramming a proprietary format tag to a standard format at the start of the ILL to help the borrowing institution.

In either the on-the-fly or systematic scenario, it is important to have all of the RFID equipment in the library upgraded to handle both proprietary and standard formats seamlessly prior to migrating the first tag. This will require close work between the library and the RFID vendor to ensure that the method of migration planned will be supported by the upgrades available. For instance, in the on-the-fly example indicated above, things will break down rather quickly if the check-in and sortation system does not support reprogramming of tags, or if it is not capable of reprogramming major classes of items such as disk media due to the characteristics of the tags and the fact that programming distances are shorter than read distances.

4.5 Libraries Currently Considering the Purchase of an RFID System (What should they require of the vendor to ensure a migration path?)

Libraries considering purchase of an RFID system in the foreseeable future should be asking their vendors to explain their planned migration path and to tell how the configuration of the equipment will allow forward compatibility with anticipated new standards. Migration plans and methods should be discussed. The most important aspect of this conversation is that the library should feel confident in the end that their investment in RFID is solid and that they will be able to use it for years into the future.

We strongly recommend that libraries only implement systems that meet these standards.

When purchasing, positive answers are needed to these questions:

1) Can I purchase tags from other manufacturers and still be sure that these new tags will interoperate with existing tags and that the existing hardware and software can be used without any (or without major) reengineering?
2) Can new hardware, such as gates or self check-out stations, work with existing tags and existing hardware?
3) Will the existing protocols and software work with the new hardware and tags? If not, what is required to make them compatible?

Caution should be taken in implementing optional proprietary features or functionality outside of the ISO/IEC 18000-3 Mode 1 air interface as they may impose limitations to later desired interoperability.

4.5.1 Emerging Technologies

Pallet and carton tagging across industries using RFID increasingly is standardizing around the Ultra High Frequency (UHF) with tag-to-reader protocols following the EPCglobal Gen 2 specification (see Appendix A). While tagging at item level has been successfully achieved with both UHF and HF frequencies, in the library application HF tags have been overwhelmingly used to date. There are several reasons for this:

1) The UHF frequency may not be as well-suited to offering EAS functionality due to its susceptibility to body shielding.
2) In the past, UHF systems only offered read ranges of several meters, making them questionable for applications such as check-out, check-in, or shelf maintenance, where shorter, more focused read ranges are preferred.
3) At the time that RFID applications were first introduced into the library market, only HF technology offered a frequency range that could be used worldwide. UHF has not completely overcome this obstacle, but progress is being made.
4) Until just a couple of years ago, tags widely available at UHF frequencies had significant issues with anti-collision performance and other technical limitations. These limitations affected the early supply-chain implementations, but again they have mostly been overcome.

Most of the above limitations on use of UHF in library applications have been overcome as the technology has evolved, with EPC Gen2, UHF near field developments, and work on frequency harmonization around the globe. Therefore it is likely that in the near future (five years or less) the UHF tags may indeed be quite prevalent in libraries.

As stated earlier, the most prevalent RFID technology in use in U.S. libraries is standardized based on ISO/IEC 18000-3 Mode 1. There is no expectation that this technology will become obsolete or cease to be useful anytime soon, but it is likely that as supply chain applications develop the technology for tracking at the item level, new standards will become available that might offer alternatives to the library market. If the performance and price of these technologies provides a compelling story to the library market, they will probably be adopted by some. These developments may occur at either HF or UHF bands, as there will likely be item-level solutions standardized at both frequencies for different applications. Additionally, adoption by libraries may be impacted by decisions made in the publishing industry, particularly in the event of source tagging by publishers, which could drive libraries to consider using tags already applied to the items they purchase.

Publishers and retailers had all but ceased to be interested in RFID technology in early 2006. In August 2006, however, subsequent to the release of the new UHF Gen2 tag, the trade press reported a successful implementation of item-level RFID tagging of books by a retail book distributor and a retail bookstore in the Netherlands and major U.S. publishers are again expressing interest in the technology, with at least one major U.S. bookstore chain actively following the roll-out of item-level RFID use in sixteen trade bookstores in the Netherlands.

It is too early to make any predictions regarding the use of UHF tags, or HF tags from an alternative standard, in libraries, but we would be remiss in not pointing out that this is a possible outcome sometime in the future.

Section 5: The Book Supply Chain

5.1 Introduction

The purpose of this section is to discuss the benefits of RFID across the supply chain of the book industry. Although RFID use in libraries is not limited to books and includes CDs and DVDs, the book supply chain is used as an example to show the benefits of implementing this technology. Publishers have taken an active role in discussing the uses of RFID through the supply chain, and members of this committee are very active in the various book industry organization. It is from this perspective that this section addresses RFID benefits and issues, as well as shows the need for a data model standard.

5.2 Book Supply Chain Overview

From its origin as ideas transferred by an author to the written page (and then edited and "designed" to create an appealing commodity), every book passes through a series of stages and status changes as it moves along the supply chain. Ideally, RFID technologies can facilitate these passages as each copy of every book follows its own odyssey from author to printer to customer.

Edited and designed (typically by a publisher), the book's physical creation is outsourced to printers and manufacturers—who are already aware that placing RFID tags in books will most likely fall to them in the future.

Once manufactured, a physical book's supply chain odyssey carries it along a branching pathway. Branches include: the printer's loading dock, shipment to a warehouse belonging to a publisher, the distributor, and/or the retail store or chain (both bricks and clicks). In some cases this occurs in sequence: publishers to distributors to retailer warehouses before ending up on the selling floor; or publisher to distributor/jobber to library; or, in some cases, from publisher to library.

In an increasing number of libraries, RFID tags are currently being applied to facilitate the cycle of library stages, including receipt, shelving, check-out, check-in, re-shelving, and eventually even interlibrary loans.

In the retail environment, a book passes through both physical and commercial stages as it moves onto the selling floor and beyond—at the most general level as a new book, a purchased book, a used book, or a book returned to the publisher.

More specifically, once in a retail environment, a book can be offered at full price, at a discount, at a deep discount, or at a remaindered price. When sold, it may be exchanged for a different title or be sold back to the retailer and then reoffered to the consumer or library as a used book. Unique to the book industry, unsold volumes of new books can be returned to the publisher, and thus retrace their steps through the supply chain for distribution to other retail outlets where demand is heavier, or simply "pulped" and returned to the raw material of paper.

Figure 1 illustrates the book supply chain.

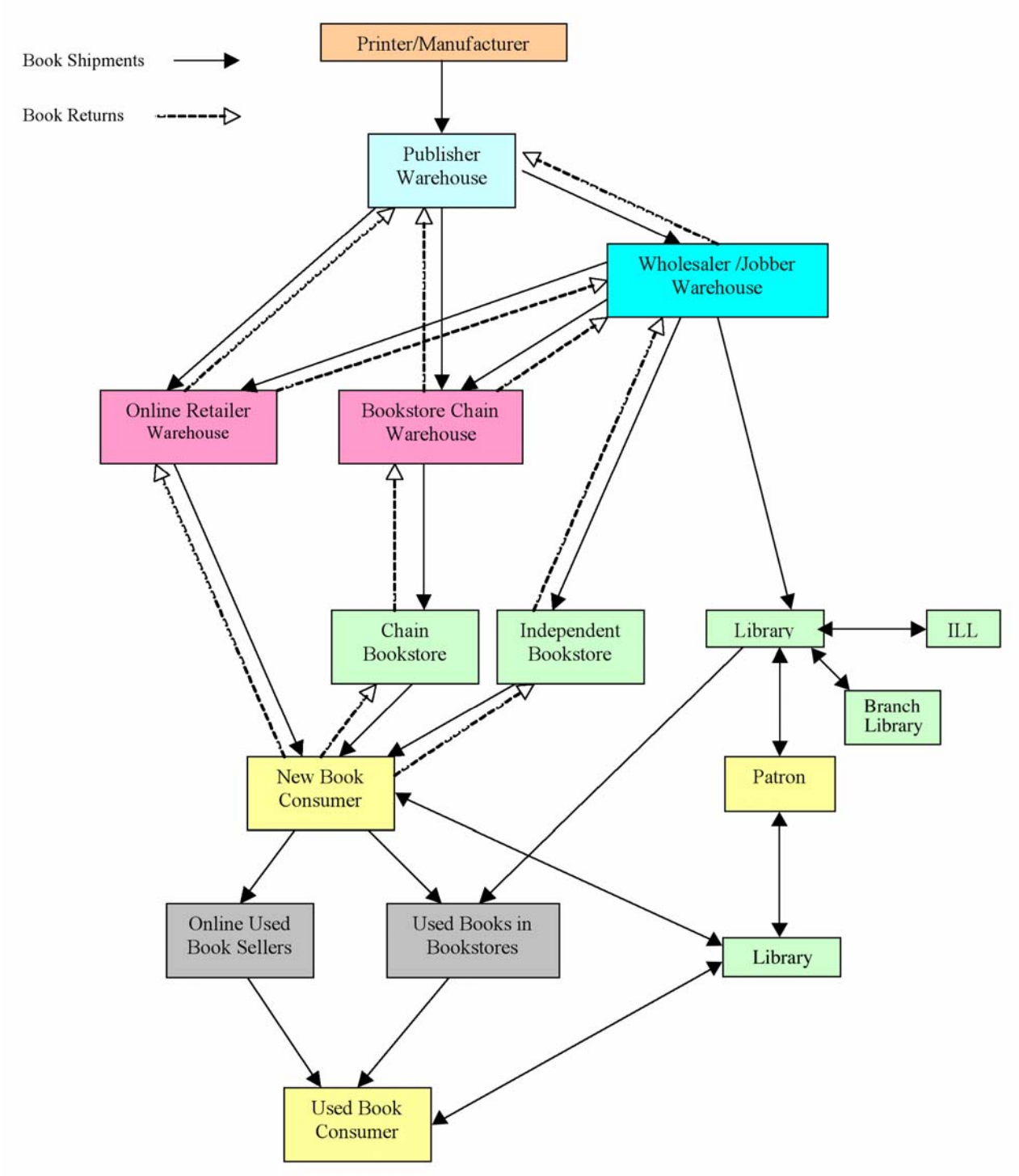

Figure 1: Book Supply Chain

5.3 RFID in the Supply Chain

The book publishing value chain—defined as publishers, manufacturers/printers, distributors, wholesalers, retailers, libraries, and related technology vendors—became interested collectively in RFID in the spring of 2003, as a result of well publicized pressure from Wal-Mart requiring that its major vendors be prepared to adopt RFID technology to tag cartons and boxes sent to a set of pilot Wal-Mart stores and distribution centers. It should be noted that major retail chains and a few publishers were aware of the technology, and that a number of libraries, e.g., New Hanover County Public Library, NC (2000) and Santa Clara, CA (2003), had already adopted early versions of RFID. Generally speaking, the library community was ahead of the rest of the publishing value chain in showing serious interest in this set of technologies.

A program about RFID, prepared for the annual meeting of the Book Industry Study Group (BISG) in September of 2003, led to the formation of an RFID working group jointly sponsored by the BISG and the American Library Association (ALA). The RFID working group decided that its first priority was the creation of a privacy policy for the book publishing industry.

Even as this privacy policy was being hammered out, problems in the commercial use of RFID tags were coming to light. These included: unacceptably high error rates during the scanning of RFID tagged boxes at the Wal-Mart pilot stores (possibly because they were using non-compliant tags), errors caused by containers of liquids and metal objects, and the inability of the corporate world to calculate a "hard ROI" that would make compliance with the "slap and ship" of RFID tags on boxes anything other than a "Wal-Mart tax." Simultaneously, anti-RFID consumer group pressure focused on the media and state legislatures grew more pointed, including one Harvard graduate student proposing, among other things, that RFID represented the "mark of the beast" as foretold in the Book of Revelations.[3]

Both the anti-RFID consumer issues and the Wal-Mart problems serve to reduce interest in RFID in the publishing and book retailing communities. But the potential benefits to libraries out weigh these concerns. Libraries adopting the technology are able to maintain patron privacy by limiting data on RFID chip to numerical item identification and using the libraries' internal secure systems. This has meant that RFID adoption is proceeding in the library community despite a number of unresolved privacy and technology issues.

By 2006, libraries were adopting RFID at a rapid pace, tagging books and other media. Publishers and retailers on the other hand, had all but ceased to be interested. In August of 2006, however, subsequent to the release of the new EPCglobal C1G2 tag (ISO/IEC 18000-6 Type C) the trade press reported a successful implementation of item-level RFID tagging of books by a retail book distributor and a retail bookstore in the Netherlands. This experiment has resulted in renewed interest among publishers and retailers.

This renewed attention from retailers and publishers will also be of interest to printers and book manufacturers. Were the book publishing industry to adopt item-level RFID technology, the publishers assume it will be their responsibility to insert RFID tags in individual books at the point of manufacture. Given the involvement of several of the larger book distributors in both retail and library operations, at least one major distributor is concerned about the lack of an industry-wide approach, including a lack of standards in both the technology and the metadata.

Watching the gradual penetration of RFID technologies in other industries and retail chains, it may be reasonably inferred that, assuming the Dutch retail book "experiment" continues to show benefits, cost savings, and efficiencies, the likelihood of adoption for book retail uses in the U.S.

[3] Albrecht, Katherine. *On the Brink of the Mark.* [S.l]: Endtime Publishing, 2004.

is growing. A cross-industry set of standards and approaches would have benefits for libraries as well.

5.4 Book Jobbers and RFID Tag Application

As libraries have been adopting RFID for theft deterrence, circulation, and inventory management, some have requested that their book jobbers apply and program tags for the new books. The state of today's proprietary RFID systems is a maze of different procedures, conversion stations, software, and tags, which makes it difficult for jobbers to cost effectively apply and program RFID. Issues include:

- costs associated with the conversion stations—the jobber must purchase a conversion station for each vendor;
- valuable space required by conversion stations in the warehouse; and
- equipment management issues—jobbers must manage the tags, and conversion stations for each RFID vendor

Figure 2 illustrates the issues facing jobbers today. The jobber is required to have a conversion stations for each library's RFID vendor. Any mismanagement of the equipment can result in Vendor A's RFID tag being applied and programmed to books for a customer needing Vendor B's tag. The condition will only be identified when the books are shipped to the customer and the RFID tags cannot be processed by their software. Figure 2 demonstrates the present requirement of multiple hardware platforms by the jobbers. There is considerable urgency on the part of the book jobber for this to change.

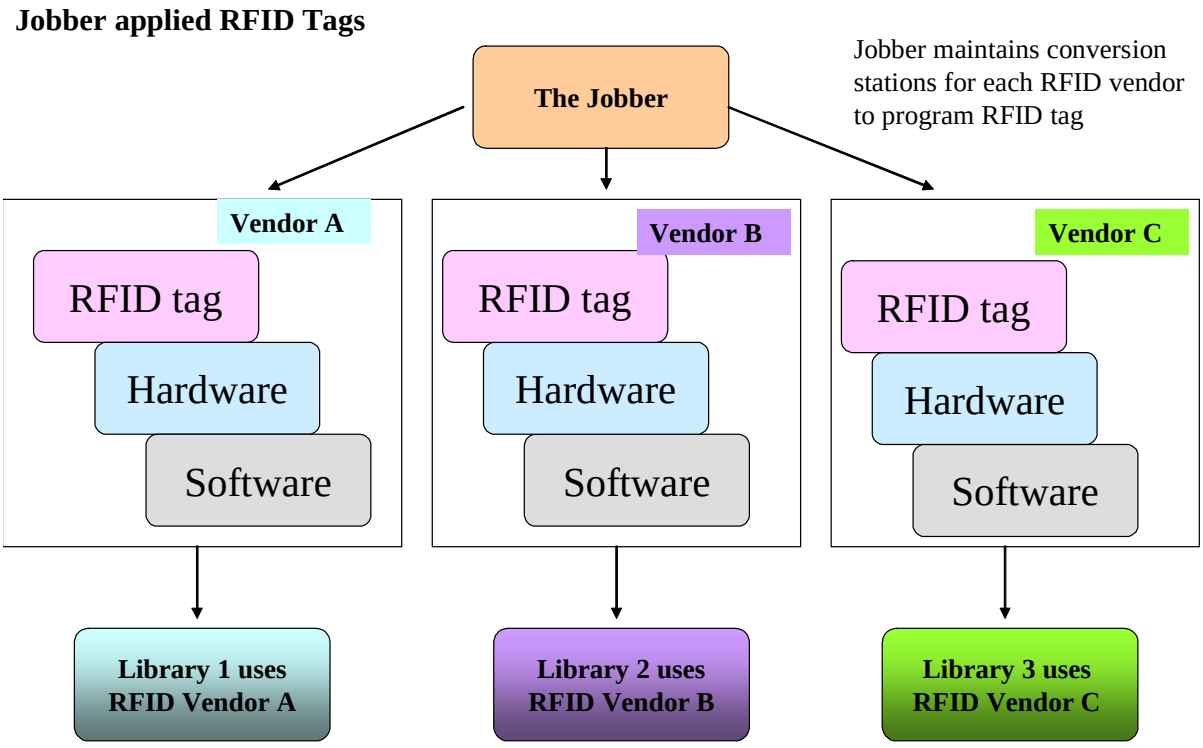

Figure 2: Jobber Applied RFID Tags

Standardization of the data model would eliminate the need for a conversion station for each RFID vendor. The movement by some vendors to the ISO/IEC 18000-3 Mode 1 standard has improved the customer/tag matching process, but the conversion station issue remains.

Figure 3 illustrates how the use of a standardized data model and the installation of the RFID chip at manufacture time simplify the programming process. Standardization will enable the jobber to easily program the RFID chips independently of the RFID vendor.

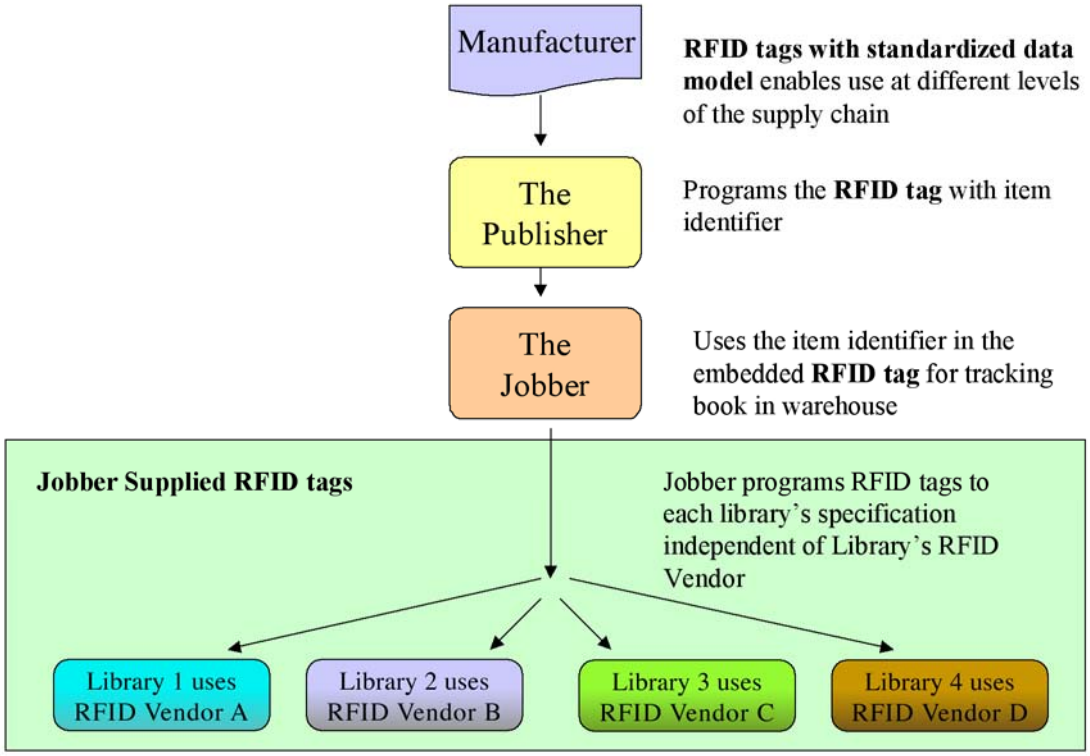

Figure 3: Standardized Data Model

In summary, until a standard data model is developed and an interoperable RFID market emerges, it will remain difficult for book jobbers to cost effectively satisfy the demand for applying and programming RFID tags for libraries. The jobber represents only one step above the library in the supply chain. It is the hope of the NISO RFID Working Group that over time the book industry will see its way to have these tags (or similar standards-based tags) applied sooner in the supply chain perhaps at the manufacturing level. The end goals of standardization include:

- reduction of equipment proliferation,
- less costly work processes,
- simplification of work processes,

- improved ROI for publishers, wholesalers, and jobbers adopting RFID in the supply chain, and
- consistent functionality of RFID from whatever point it is applied to the media, through the supply chain to circulation in libraries.

Section 6: Privacy

6.1 Privacy Issues

It is all but impossible to separate out privacy issues from all other aspects of RFID when analyzing the uptake of these technologies for consumers and citizens in the United States. Many factors have created this tangled situation, including:

- The absence of well established, generic privacy policies like those dating back to the 1980s in Europe, which give consumers/citizens a sense of confidence about protection of personal information.
- An atmosphere of less regulated capitalism in the U.S., as well as early RFID pilots in retail environments that were poorly explained and thus publicly distressing.
- The Patriot Act, which noticeably reduced the appearance and reality of personal privacy from government "snooping."
- Technophobia in general.
- The promotion of RFID by large and trendsetting organizations like Wal-Mart and the United States Department of Defense.
- Spurred by consumer groups like the Electronic Freedom Foundation (EFF), the press initially focused on the more drastic potential for violation of individual privacy. As public experience with RFID technology has grown over the past several years—thanks to use for automated highway toll payments, building access, and small transaction credit cards—media coverage has also begun to focus on consumer benefits and functionality. In covering California Governor Schwarzenegger's veto of an RFID privacy bill in October 2006, for example, the press highlighted the governor's interest in this technology "to reduce costs and improve customer service."
- In certain instances in the library community, the use of RFID as a pawn in other local and political power struggles.

It is evident that RFID is a technology that could conceivably be used to track, minutely and systematically, the movements, acquisitions, reading habits, health conditions, uses of pharmaceutical and food products, etc., of individual citizens. Thus, in the current environment, it is not surprising that RFID quickly reached a flash-point in America—despite the fact that its technological immaturity makes such Brave New World applications mostly science fiction at this point in time. Moreover, other widely used technologies like credit card purchases, cell phones, and GPS systems can already be used to track individuals effectively.

Even in private dialogues, where the reality of RFID's technological infancy was acknowledged by consumer advocates, groups like EFF posited a general problem of privacy pollution and erosion that RFID, even if relatively benign in its current manifestation, would only exacerbate.

Curiously, in those instances where RFID has simply been adopted in the U.S., but *not* identified as such, the technology has been accepted without much complaint or concern. For example:

- EZ-Pass (for automobile toll collection),
- Speed Pass (to buy gasoline and other products at Mobil gas stations), and
- "express pay" credit cards from VISA and other credit companies.

In its early days, RFID is clearly a case where "perception is reality," which is typical of the introduction of any new and potential world-changing technology, whether electricity or the Internet. Time is needed for public familiarization, a clearer understanding of benefits versus risks, and user experience, which, as always, are the factors that will lead to comfortable implementation or sustained resistance to RFID.

6.2 EFF Position on RFID and Personal Privacy

One of the most articulate and thoughtful of the consumer groups, the Electronic Frontier Foundation, makes the following statement about RFID on its website:

> Libraries, schools, the government, and private sector businesses are adopting radio frequency identification tags, or RFIDs—a technology that can be used to pinpoint the physical location of whatever item the tags are embedded in. While RFIDs are a convenient way to track items, they are also a convenient way to do something far less benign: track people and their activities through their belongings. EFF is working to prevent the embrace of this technology from eroding privacy and freedom.
>
> Electronic Frontier Foundation: *RFID*
> Retrieved February 20, 2007, from
> http://www.eff.org/Privacy/RFID/

Among EFF's priorities is to keep what they term as "privacy-leaking" chips out of California state IDs.[4] Note that their position, as stated above, is not to eliminate the use of the technology, but to "prevent the embrace of this technology from eroding privacy and freedom." This position of protecting privacy is whole-heartedly shared by all libraries.

6.3 ALA/BISG Initiative

In 2003, a variety of technical, economic, and social issues were of concern to the members of the RFID working group sponsored by the American Library Association/Book Industry Study Group (ALA/BISG)—including representatives from libraries, publishers, retailers, wholesalers, distributors, and technology vendors. What moved the group to action was the potential for negative public reaction to RFID due to the possibility of unwarranted government intrusion, particularly in the era of the USA Patriot Act. The explicit goal of crafting a formal policy was to "get out in front of the privacy issues" in advance of any general implementation of RFID in the book publishing value chain. In the view of the ALA/BISG working group, RFID is a set of technologies that has the promise to provide multiple and significant benefits to the entire

[4] See the August 31, 2006 news release "California Lawmakers Pass Safeguards for Privacy-Leaking RFID Chips" at http://www.eff.org/news/archives/2006_08.php. This matter is also the only item listed under the "Take Action" portion of the EFF's RFID site: http://www.eff.org/Privacy/RFID/. See also: http://www.cla-net.org/included/docs/IT3.pdf

industry. Underlying the group's work, moreover, was a realization that these technologies will continue to evolve and thus any policy should avoid technological specifics and remain at a level that will still be relevant as the technology moves forward.

Completed in late 2004, and subsequently adopted by BISG and ALA, the privacy policy recommendation has five main tenets.

> All businesses, organizations, libraries, educational institutions, and non-profits that buy, sell, loan, or otherwise make available books and other content to the public utilizing RFID technologies shall:
>
> - Implement and enforce an up-to-date organizational privacy policy that gives notice and full disclosure as to the use, terms of use, and any change in the terms of use for data collected via new technologies and processes, including RFID.
> - **Ensure that no personal information is recorded on RFID tags which, however, may contain a variety of transactional data.** [Emphasis added.]
> - Protect data by reasonable security safeguards against interpretation by any unauthorized third party.
> - Comply with relevant federal, state, and local laws as well as industry best practices and policies.
> - Ensure that the four principles outlined above must be verifiable by an independent audit.
>
> *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles*
> Adopted by the ALA Council January 19, 2005

6.4 A Technology Perspective on Privacy Concerns

The following points are important to understand about today's RFID technology in the library environment:

RFID tags in libraries are powerless.

RFID tags come in many varieties. The tags that are presently used in libraries are 13.56 MHz (megahertz) tags with no embedded power source. The tags are literally "powerless." Without power, the tags can do nothing; they are inert and inactive. The tags receive their power from an antenna (or reader). When a reader comes in close proximity (say within 2 to 18 inches) of a tag, then the tag is temporarily charged and becomes a very small radio that begins to transmit its data. There are no batteries in the tag to store any power. So when the antenna goes out of range, the tag once again becomes inert and inactive. Thus, any exposure to privacy issues can only happen in the presence of an antenna that is within a very close range of the tag. Clearly, the concept that someone driving by your house with an antenna or that a satellite passing overhead will energize these tags is ignoring the reality that the antenna or satellite would have to be within inches of the item. At that distance, it would probably just be easier to read the title on the cover of the book, rather than scan the item for its ID number, which would only be relevant with access to the information contained in the owning library's presumably secure database.

One might argue that future tags may have a power source associated with them. Indeed, today RFID tags used in some applications do have integral power sources and are termed "active

tags." But for library applications, this has two problems. First, power requirements within the tag would increase the price and size of the tag substantially. Second, batteries are sure to run out, seriously limiting the useful life of the tag—defeating the whole purpose of it. Therefore, we expect that even in the future the RFID tags in libraries will be "powerless" and with very limited read ranges, thus seriously limiting the damage they can do to privacy.

RFID tags used in libraries have a very short read range.

The read/write range of HF RFID tags is limited. These tags operate at 13.56 MHz in a magnetic field created by the RFID reader. This field drops off rather quickly, and does not propagate in the manner of electric field transmissions used with RFID tags in the UHF range. Because the communication between the reader and the tag is based on the coupling strength between their antennas, the range at which a tag can be read is primarily determined by the size and design of these antennas, and the amount of power generated by the reader. Most library desktop applications of RFID utilize reader antenna designs which will produce read ranges of 8–12 inches with commonly sized HF RFID tags, with tag antennas in the 2x2- or 2 x 3-inch ranges. This is quite intentional. If the range were large, then there would be increased risk of interference with other tags in the area. Certainly, we do not wish to inadvertently check-out a room full of books to a single patron when our intent is to check-out a single book or just a few items.

Library applications that require more range—such as security gates that must read tags within the corridor while maintaining a 36-inch aisle for comfort and to meet ADA guidelines—are typically designed to produce 20+ inches of read range from each pedestal with the same tags as above. This is accomplished by using pedestal antennas with geometries and sizes that maximize the field strength within the corridor and by applying higher power levels, sometimes as much as 4 watts, to these antennas.

In the retail industry there are some RFID tags, typically in the UHF frequency range, which have a much larger read range—up to tens of feet—and this range is obtained with relatively small reader antennas. This is not the case with the HF tags used in libraries. For these tags, the shorter, more defined reading zone afforded by HF technology has several advantages. Privacy risks can be minimized due to the limited read range. Also, potential interference between adjacent readers can be minimized. Further, the risk of unintentional reading of tags in the vicinity of reader stations can be reduced.

This is one area where it will be desirable, in the future, to ensure that the read range of tags for library applications is not substantially increased over the present range of 8 to 20 inches.

Section 7: Vandalism

7.1 Introduction

Vandalism has long been an issue for organized societies, with many attacks made, for example, on public property as a statement against government or other authority. Libraries have been the targets of vandals for years, with assaults ranging from censorship (criminally defacing or destroying materials that one does not wish to be publicly available) to wanton destruction of library materials or facilities, to outright arson. RFID technology itself presents an opportunity for vandalism that we will describe in this section.

There are several sources of potential help with preventing the various attacks available to vandals. First and perhaps most basic, most societies provide for criminal penalties against the perpetrators of vandalism, if they can be identified and prosecuted. Of course, there is an expense involved in the prosecution of such cases, both in time and financial resources.

Technology can provide some impediments to the vandal, such as that offered by password protection schemes on data that must remain changeable during the life of the item, simple locking on static data, and perhaps other methods in the future. Ultimately, most of these schemes create difficulties in implementation and hinder interoperability, and place the library only a few steps ahead of increasingly sophisticated vandals.

Libraries must ultimately choose whether the impediments presented to vandals outweigh the detrimental impacts of the protections, keeping in mind that traditional low-tech methods remain available to vandals. Different libraries will find the balance point in different positions on this issue, and there is really no right or wrong choice for libraries to adopt. For many libraries, the least expensive solution may be to accept the basic risks associated with RFID as an incremental difference over the exposure they encounter just by maintaining their collections with open doors.

Given that libraries are finding benefit from RFID systems, we recognize that these systems are vulnerable to electronic vandalism. Many RFID tags allow the modification of portions of tag memory if these portions are not locked or otherwise permanently programmed. A sufficiently sophisticated vandal has a number of attacks available, which fall into two basic categories: modification of security data and modification of tag contents. This section describes some of the potential attacks that a vandal might make on a library RFID system.

7.2 Modification of Security Data

In this attack, a criminal uses an RFID reader to modify the security information on a tag in order to steal an item or perpetrate a malicious act. Tagged materials can be stolen from the library by programming security data to the “off state” with a RFID reader. An individual with malicious intent could use the RFID reader to permanently turn off security by locking the security data. This may be accomplished on tags and systems using AFI or an EAS method for security. Virtual deactivation is not susceptible to this type of vandalism.

7.3 Modification of Tag Contents

In this attack, the criminal uses an RFID reader to reprogram the contents of the RFID tag for purpose of vandalism or theft. This could include programming random data, erasing data, or locking data for malicious purposes. Data can also be changed to valid but incorrect data for the purposes of theft, i.e., exchanging item numbers. Any of these situations causes difficulty to the library. Programming and locking the primary item identifier (see Section 2.5.1 for definition and explanation) will enable the library to protect against modification of tag contents. Data objects that have been altered may be able to be reconstructed, as long as the primary identifier is still intact.

7.4 RFID Viruses

There has recently been some discussion of theoretical attacks on RFID systems using what have been called "RFID viruses." In these attacks, a particular data string is encoded on an RFID tag, and that tag is presented to the victim system. If the system design allows, the data on the tag might be read by the system and cause it to do something damaging or destructive, and/or, as the name suggests, something that would cause the virus to spread.

The debate over RFID viruses was lively for a period of time, with some parties arguing that this was a tremendous vulnerability of systems, and others arguing that the vulnerability exists only if specific design features are implemented to make it credible. [5] The latter argument suggests that the theoretical threat can be realized only if systems are intentionally designed to be susceptible to such attacks. For the present discussion, let's assume that the threat is real but manageable and focus on the practical aspects.

As described in papers on the subject, typical spreading of the virus is accomplished by writing the virulent data into other tags encountered by the system. This might be accomplished by modifying a data object in a system to include a command embedded in the tag to define the information to be written to tags programmed by the system. Other destructive actions that could be caused by a virus include undesired operations on the system triggered by commands embedded in the data on the infected tag—for instance, the tag could contain a command directing a database to delete a table of data.

Compliance with standard encoding schemes can, to some extent, prevent such an attack. At this writing, we are aware of no such attacks against existing library RFID systems. Prudent system designers have guarded against creating designs that are susceptible to attacks such as these in the past, and with disclosure of this threat we expect systems to be further hardened against such attacks.

7.5 Physical Defacing or Removal of the Tag

The most widely available and low-technology method of vandalizing an RFID implementation on a library item is simply to remove or mutilate the RFID tag itself. To date, this has been recognized as a fairly minor issue in library implementations, but it does exist, just as such attacks have existed for barcodes and other item labels. If the industry begins to incorporate RFID tags into the construction of library items, the tags might become less susceptible to this kind of attack because they may be less visible and thus more difficult to damage the tag

[5] See "The Industry Reacts to RFID Virus Research," *RFID Update: The RFID Industry Daily*, March 20, 2006, http://www.rfidupdate.com/articles/index.php?id=1077.

without obviously damaging the item. Short of changes such as this, the tags remain visible and accessible to the vandal.

7.6 Intentional Detuning of the Tag

The low-tech method of defeating the security functionality is simply to shield or detune the tag, by means of tin foil or a commercially produced tool marketed to provide privacy for consumers. Such techniques have also been publicized as a means for travelers to protect their privacy amidst threats against electronic passports.

7.7 Moving Forward

It is not the intention of the Working Group to scare potential users away from embracing this technology by exposing it obvious limitations. But, rather, the Working Group feels strongly that the benefits of the technology far outweigh the limitations that it brings with it. Over time, the technology will improve and erase some of these limitations. Similarly, over time, vandals will discover newer techniques to defeat the security of these systems. The Working Group is of the unanimous opinion that libraries should move forward with the implementation of this technology when funding permits and do so with the full understanding of the benefits and limitations that come with it.

For additional readings on vandalism, see the Bibliography.

Appendix A
RFID Technology Basics

A.1 What Is RFID?

Radio Frequency Identification (RFID) is an automatic identification and data capture technology. RFID systems use radio waves as the communication medium between RFID tagged objects and RFID reader stations. Tags—or "electronic labels," as they are also known—operate as portable databases that can be accessed wirelessly. The memory on these tags can be read and written to remotely and at very high speed.

RFID, though relatively new to libraries, has been in existence for more than sixty years, and it has been extensively used in applications such as toll collection, access control, ticketing, and car immobilization devices (also called immobilizers). In recent years, the technology has received increased attention due to a confluence of actions, including technology advancement, heightened security concerns, supply chain automation, and a continuing emphasis on cost control within industrial systems. The technology offers a revolution in the efficiently of item management and traceability.

The primary benefit of RFID tags over barcodes is their ease of use and reliability. RFID tags can be read while in motion, in any orientation, through intervening objects and without the need for line of sight. RFID tags enable reliable automation, while barcodes are better suited for manual scanning. Perhaps most significant is the fact that several RFID tags can be read simultaneously and automatically, while barcodes have to be scanned one by one. Though it is a costlier technology compared with barcodes, RFID has become indispensable for a wide range of automated data collection and identification applications that would not be possible otherwise.

A.2 How Does RFID Work?

A typical RFID system is composed of three key components—a reader, tag(s), and a host computer.

The RFID reader sends out electromagnetic waves in the RF (Radio Frequency) spectrum. When the tag enters the RF field, the tag's electronic circuits are powered by energy from the RF field. The tag then modulates the waves and the sends them back to the reader. The reader converts the signals received from the tag into digital data and sends it to the host computer.

More specifically, the key RFID system components are described below:

> **An RFID tag** consists of an integrated circuit (IC) attached to a tag antenna. The IC is the heart of the tag. The electronic circuits on the IC define the functionality and memory capability of the tag.
>
> The tag antenna is a conductive structure specifically designed to couple or radiate electromagnetic energy. The shape and size of the antenna dictate the RF tag operating frequency and the read range of the desired system. The antenna is typically fashioned

via electrochemical etching or deposition techniques or in some instances can be manufactured using conductive ink printing.

The base material of the tag is often polyester, PET, and other plastic films, but can also be paper substrates.

RFID tags come in a multitude of form factors and packages. They are available in a variety of sizes, shapes, and degrees of rigidity, robustness, and flexibility to fit with the item it is intended to identify, along with the reader performances expected at each transaction stage. These include thermal transfer labels, plastic cards, key fobs, or encapsulated buttons. Tags can also be incorporated or even embedded into materials such as cardboard, plastic, wood, textiles, or the living tissues of animals or humans.

An RFID Reader Station is made up of an RFID reader and an antenna. It can read information stored in the RFID tag and also update this RFID tag with new information. It generally holds application software specifically designed for the required task. RFID stations may be mounted in arrays around transfer points in industrial processes to automatically track assets as they are moving through the process.

An RFID reader station can be fixed or handheld, and is usually connected to management information system or host computer.

Reader antennas are available in a variety of shapes and sizes; they can be built into a door frame to receive tag data from persons or things passing through the door, or they can be mounted into EAS gates; embedded into desk tops and other furniture; or integrated into conveyer or other materials-handling systems.

The electromagnetic field produced by an antenna can be constantly present when multiple tags are expected continually. If constant interrogation is not required, the field can be activated by a sensor device.

Readers may operate at different RF frequencies, and even within a single frequency they may still use different communication protocols. Air interface protocols are the rules that govern how tags and readers communicate.

Two common families of protocol are Reader Talks First (RTF) and Tag Talks First (TTF) protocols. For RTF systems the tags wait to be commanded to communicate data and signals by the reader. For TTF systems, tags send information continuously while in the RF field and powered up, without waiting for a specific command from the reader.

A.3 What Are the Frequencies Used?

RFID technology can be implemented using different radio frequencies to wirelessly communicate data and commands to and from the RFID tag from the RFID reader. The different frequencies offer different properties and features. The choice of frequency for a given application will depend on the requirements of the application and the best match of these requirements to the frequency properties.

There are four key RFID frequencies bands used today:

Low Frequency (LF) 125 - 134 KHz. LF is mostly considered for specific applications, although its deployment is global. It has minimal metal interference and is not sensitive to the presence of water. Expected read range is below 1.5 meters, with low data transmission rates. This carrier frequency is dominantly used for animal identification, vehicle immobilizer systems, and no-contact “proximity” access control.

High Frequency (HF) 13.56 MHz. HF is widely deployed, thanks to a broad global frequency deployment. It is minimally affected by moisture and uses higher data transmission rates than LF. Read range is below 1.5 meters. Manufacture of HF tags can be achieved using very low-cost, reel-to-reel processing techniques, offering low-cost tags. The frequency is highly reliable and predicable in the presence of metals and for random tag orientations. Main applications are for asset tracking applications, such as library automation; laundry process automation; courier- and item-level supply chain; and retail tagging applications.

Ultra High Frequency (UHF) 860 - 960 MHz. UHF is less globally harmonized for frequency and power regulations than LF and HF, although initiatives by EPCglobal are improving this situation. Currently, different countries have different UHF frequencies available for RFID, and different power levels available. The UHF frequency offers greater read range than other frequencies, but is adversely affected by moisture and cannot read tags shielded by the human body. The presence of metal also creates reflective surfaces that can dramatically degrade the performance of these systems. UHF antennas are tuned to receive RFID waves of a certain length from a reader, just as the tuner on the radio in a car changes the antenna to receive signals of different frequencies. When UHF antennas are close to metal or metallic material, the antennas can be detuned, resulting in poor performance. The main applications for UHF are pallet and case tracking for supply chain logistics and vehicle tracking; however, some item-level applications are being implemented and industry groups are considering additional applications.

Microwave 2.45 GHz. Another frequency being used for RFID is the microwave 2.45 GHz frequency. This frequency is more globally available than UHF, but is totally unsuitable in the presence of liquids, which absorb this frequency. The frequency is not widely deployed and requires complex implementation. Primary use is vehicle access control.

The physics of the interaction between reader and tag at LF and HF are very different to the interaction between reader and tag at UHF and microwave. At the lower frequencies (LF and HF), the physical mechanism for the data communication is transformer-type electromagnetic coupling and energy is transferred from the reader to the tag and vice versa by virtue of mutual inductance between their respective antennas. Whereas at the UHF and microwave frequencies the electromagnetic field operates in a radiating or propagating wave, the energy for LF and HF is radiated by the reader and reflected by the tag antenna.

This difference in physics fundamentally defines the different characteristics of the various RFID operating frequencies.

Of the four frequencies mentioned above, the two that are likely to offer the best low-cost, high-performance features and are best suited to mass-volume applications are HF and UHF.

When considering a carrier frequency, it is important to consider worldwide regulations that determine whether this frequency is usable all around the world or only in specific parts or regions. FCC, ETSI and Japanese emission limits are very similar for 13.56 MHz and 125 kHz. It allows the use of one unique RFID system reliable all over the world.

UHF normalization is still in progress: different frequencies are currently used, different power levels apply, and different communication modes exit. Considerable efforts to harmonize UHF are in progress, but a fully harmonized environment is unlikely in the near future.

A.4 Types of RFID Tags

Passive

There are many varieties of RFID, but the most common is passive RFID systems. Passive tags have no battery or other power source on the tag; they must derive all the power required for their operation from the reader's electromagnetic field. Passive tags consequently tend to be flat, in label form, are low in cost, and offer a virtually unlimited operational lifetime. The tradeoff is that they have shorter read ranges than battery-powered tags.

Active

An active RFID tag is one that has a transmitter to send back information, rather than reflecting back a signal from the reader as a passive tag does. Most active tags use a battery to transmit a signal to a reader. Active tags can be read from 300 feet (100 meters) or more, but they tend to be expensive (typically more than US $20 each, in 2007). These tags are primarily used for tracking expensive items over long ranges. For instance, the U.S. military uses active tags to track containers of supplies arriving in ports. EZPass toll collection systems are also based on active tags.

Sensor

Sensor tags incorporate sensors as well as memory on the tag. RFID sensor tags for measuring air pressure in car tires or temperatures for cold food and drug monitoring are becoming more widely used.

A.5 Memory Capacity and Functionality

There are two main types of tag memory structure: Read Only and Read/Write. Read Only is the term applied to a tag in which data is written (or programmed) once during manufacturing, and afterwards can only be read and but not changed or altered in any way. Read/Write is the term applied to RFID tags that can be written (or programmed) and can subsequently be rewritten and reread numerous times.

There is a third field-programmable structure that is also of the read/write variety. After having been programmed by the user, this Write Once/Read Many (WORM) structure accords the user the ability to lock the tag's memory indefinitely.

Read Only tags are typically passive and are programmed with a unique set of data (usually 32 to 128 bits) that cannot be modified. Read Only tags most often operate as a license plate in a database, in the same way as linear barcodes reference a database containing modifiable, product-specific information.

A.6 Constraints Related to RFID Particularly Relevant to Libraries

When implementing RFID solutions it is necessary to recognize some of the physical constraints of the technology. There are two areas that should be considered and are particularly relevant to library applications. Firstly, the presence of metals in the RFID reading environment and, secondly, the placement of RFID tags relative to each other.

Communication between RFID readers and tags occurs via electromagnetic waves operating in the Radio Frequency spectrum. The communication is governed by the laws of physics related to RF propagation. If metal is placed between the tag and reader, communications can be

broken, as metal is impervious to RF waves. Care should particular be taken in a library environment when tagging books with metal foil covers. Also, care should be taken to avoid tags being placed flush with the end of metal book shelves.

Placement of currently deployed high frequency (HF) tags is a critical factor affecting system performance (see Figure 4 below). When tag placement in one item directly overlays another placement and both items are in very close proximity, readability is compromised. The antenna component of each tag interacts and changes the radio frequency, making it difficult for the RFID readers to communicate with the tag. This is analogous to tuning your FM receiver just a little bit away from the channel you are trying to receive, diminishing the quality of the reception. A way to avoid this is the process of staggering tags in like items that are shelved in close proximity.

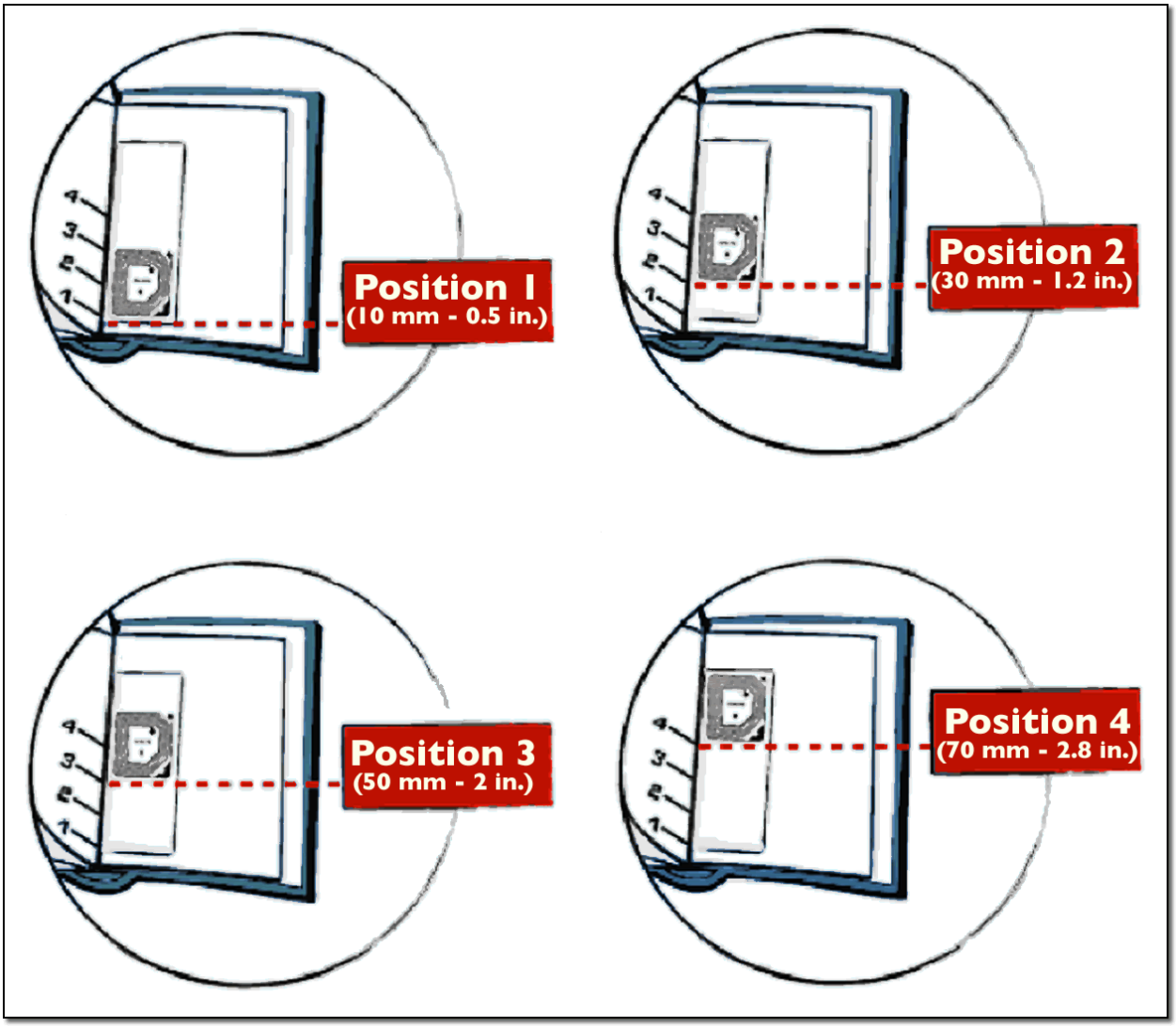

Figure 4: Placement of HF RFID Tags

While RFID tags operate with high reliability and readability on most items, principally books, there are still challenges in regards to some forms of media. Size constraints and presence of metal are core issues to overcome. These constraints apply equally to all applications of RFID.

A.7 ISO Standards

Standardization is a complex area. There are a myriad of standards groups (international, national, and industrial) generally denoted by acronyms. For example, just a few are IATA, CEN, ETSI, ANSI, AIAG, and ISO, and the list goes on. This alphabet soup is further complicated by an apparently random numbering of standards. To understand the RFID standardization environment, some structure and simplification is required. Amongst the numerous standards groups there are two key bodies driving the RFID standardization process. These are EPCglobal and ISO.

EPCglobal Inc. is an industry standards group comprising end-user companies and technology suppliers. As a joint venture between GS1and the Uniform Code Council® (UCC®), EPCglobal's objective is to drive the global adoption and implementation of the Electronic Product Code (EPC) network across industry sectors. The EPC network will enable total asset visibility within industry and retail logistics supply chains. RFID is seen as a key facilitating technology for the EPC network and, as such, is one focus of the standardization activities of the organization. EPCglobal has published an RFID UHF standard known as Gen2, and is currently in the process of developing a HF specification.

International Organization for Standardization (ISO) is, as its name suggests, is an international standards body. It is the world's largest developer of standards, and is a non-governmental organization that works with representatives from 147 countries to define standards for technology. ISO has been developing standards for RFID for over eight years.

The International Standards Organization has published the ISO/IEC 18000-3 standard jointly with the International Electrotechnical Commission (IEC). This is the most comprehensive RFID standard available today.

This standard is a technology standard that defines:

- the physical interface between the RFID tag and the RFID reader (i.e., RFID operating technology, data-encoding techniques, and the communication data rate);
- a limited number of standard commands (e.g., wake up, read); and
- the algorithm to enable communication with several RFID tags located in a single read zone (multi-read mechanism: read/write all at once).

However, this standard does not define the criteria that are specific to a particular application and have a fundamental impact on the overall RFID system's performance:

- size and shape of the tag antenna;
- security function;
- memory size (too much data stored in tags would slow down applications);

- memory structure (i.e., data formats, read-only, read/write, write once/read many, lockable parts); or
- specific commands, such as faster writing or reading. RFID chip vendors will be free to implement additional custom commands to enhance the performance of their RFID systems.

Appendix B
Interoperability Characteristics

Table 2 considers the interoperability of a tag in an interlibrary loan situation, based on security characteristics of the systems in use.

Table 2: Interoperability in ILL Based on Security Characteristics

ILL Example		Borrowing Library Equipment Uses:			
		AFI Used for Security	EAS – Vendor 1 (also supports AFI for application separation)	EAS – Vendor 2 (also supports AFI for application separation)	Database Lookup (also supports AFI for application separation)
Owning Library Tag and Equipment Uses:	Tag Supports AFI (no tag support for EAS)	Seamless interoperable security	EAS feature will not work for this tag. Item security will not be available at borrowing library.	EAS feature will not work for this tag. Item security will not be available at borrowing library.	Interoperable security after database update adds borrowed item at borrowing library
	EAS – Vendor 1 (tag also supports AFI)	Seamless interoperable security	Seamless interoperable security	EAS feature will not work for this tag. Item security will not be available at borrowing library.	Interoperable security after database update adds borrowed item at borrowing library
	EAS – Vendor 2 (tag also supports AFI)	Seamless interoperable security	EAS feature will not work for this tag. Item security will not be available at borrowing library.	Seamless interoperable security	Interoperable security after database update adds borrowed item at borrowing library
	Database Lookup (tag also supports AFI)	Seamless interoperable security	EAS feature may work for this tag, if the tag supports Vendor 1 EAS. Otherwise item security will not be available at borrowing library.	EAS feature may work for this tag, if the tag supports Vendor 2 EAS. Otherwise item security will not be available at borrowing library.	Interoperable security after database update adds borrowed item at borrowing library

Legend
Seamless security interoperability
Interoperable security for some but not all libraries
Interoperable security with operator intervention
Security not interoperable for this case

Some explanation is required to explain the different sections of this table. Several assumptions must be made by the reader. Some of these assumptions are listed here: In the table, EAS Vendor 1 and EAS Vendor 2 are assumed to use incompatible and proprietary EAS designs. If two EAS vendors use a compatible EAS design, then libraries using systems from these two vendors should be interoperable for security.

It is worth explaining the meanings of the different compatibility areas on the table as well.

1. Seamless Security Interoperability

These sections of the table are characterized by either totally compatible security mechanisms, where the lending library uses precisely the same RFID security technology as the borrowing library, or where the borrowing library uses a security method that is supported by the tag on the borrowed item.

Examples:

- The lending library uses AFI for security, and the borrowing library uses AFI for security. A tag that supports AFI will provide security at the borrowing location.
- The lending library uses EAS from Vendor 1 or Vendor 2 for security, but the borrowing library uses AFI for security. A tag that supports AFI will provide security at the borrowing location.
- The lending library uses database lookup for security, and the borrowing library uses AFI for security. A tag that supports AFI will provide security at the borrowing location.
- The lending library uses EAS from Vendor 1 for security and the borrowing library also uses EAS from Vendor 1. A tag that supports this method of EAS will provide security at either location.
- The lending library uses EAS from Vendor 2 for security and the borrowing library also uses EAS from Vendor 2. A tag that supports this method of EAS will provide security at either location.

2. Interoperable Security with Operator Intervention

These sections of the table are characterized by compatible security technologies that require some kind of operator intervention to interoperate. For example:

- If the lending library and the borrowing library both utilize a database lookup system and if the database information for an item in the lending library can then be sent to the borrowing library, the borrowing library will be able to secure the item.
- If the lending library uses AFI or any tag-based EAS method (i.e., relies on an EAS function built into the tag design), it is still possible to use the database lookup method to provide security for the item at the borrowing library. In that case, however, the borrowing library database must be configured with that item, either manually or by loading records from the lending library.

3. Interoperable Security for Some but Not All Libraries

These sections of the table identify situations where the viability of providing item security in the borrowing library depends on the particular tag technology used. For example:

- If the lending library uses database lookup for security and uses tags from EAS Vendor 1 and, if the borrowing library uses EAS from Vendor 1 for security, the tag will then provide security in the borrowing library. If, on the other hand, the lending library uses tags from EAS Vendor 2, then the security system at the borrowing library will not function with the tags.
- Likewise, if the lending library uses database lookup for security and uses tags from EAS Vendor 2, then if the borrowing library uses EAS from Vendor 2 for security the tag will provide security in the borrowing library. If, on the other hand, the lending library uses tags from EAS Vendor 1, then the security system at the borrowing library will not function with the tags.

4. Interoperable Security for Some but Not All Libraries

These sections of the table identify situations where the security system at the borrowing library will not secure the tag used by the lending library. For example:

- If the lending library uses AFI for security and uses tags that do not include an EAS function, then an EAS-based security system at the borrowing library will not provide security for an item tagged by the lending library.
- Additionally, if the lending library uses tags that include an EAS feature from Vendor 1, but the borrowing library uses incompatible EAS-based security systems from Vendor 2, then the system at the borrowing library will not provide security for an item tagged by the lending library.
- Likewise, if the lending library uses tags that include an EAS feature from Vendor 2, but the borrowing library uses incompatible EAS-based security systems from Vendor 1, the system at the borrowing library will not provide security for an item tagged by the lending library.

Appendix C
Comparison of USA-NISO and Australian Data Models

NISO Data Object Description	NISO Relative OID (Likely to Change)	NISO Length Definition	NISO Category	Australia Data Object	Australia Category
Primary Item ID (unique item identifier—UID)	01	Variable Expected: 16 bytes	Mandatory	Primary Item ID	Mandatory
Tag Content Key	02	Variable	Mandatory	Not Used	—
Owner Library/Institution	03	Variable Max: 16 bytes	Optional (1)	Owner Institution	Optional
Set Info (number of parts; ordinal part number)	04	Fixed 1 byte	Optional (2)	Set Info	Optional
Media Format	05	Fixed 1 byte	Optional (3)	Media Format	Optional
Type of Usage – Circulating? Reference?	06	Fixed 1 byte	Optional (4)	Type of Usage	Optional
Shelf Location	07	Variable Expected: 16 bytes	Optional (5)	Not Used	—
ILL Borrowing Institution	08	Variable Max: 16 bytes	Optional (6)	Not Used	—
ILL Transaction ID	09	Variable Expected: 9 digits	Optional (7)	Not Used	—
GS1 Identifier (Includes ISBN)	10	Variable Max: 13 digits	Optional (8)	Not Used	—
Title	11	Variable Expected: 32 bytes	Optional (9)	Title	Optional
Supply Chain Stage	12	Fixed 1 Byte	Optional (10)	Not Used	—
Supplier Item ID (alternate Item ID)	13	Variable Expected: 16 bytes	Optional (11)	Secondary Item ID	Optional
Local Data –1	14	Variable Expected: 10 bytes	Optional (12)	Not Used	—
Local Data –2	15	Variable Expected: 10 bytes	Optional (13)	Not Used	—
Order Number	16	Variable Expected: 12 bytes	Optional (14)	Order Number	Optional
Invoice Number	17	Variable Expected: 16 Bytes	Optional (15)	Invoice Number	Optional
Supplier Identification Data	18	Variable Expected: 32 bytes	Optional (16)	Supplier ID	Optional
Not Used	—	—	—	Usage Qualifier	Optional

Appendix D
Codes for Media Format

The following table is a suggested list of codes for the Media Format element. (See Section 2.5.5.) This list was extracted from the ONIX Books Code Lists, Issue 7, March 2007, List #7, Product Form Code.

Code Value	Code Description	Notes on the meaning and the usage of the code
	Undefined	
AA	Audio	Audio recording - detail unspecified
AB	Audio cassette	Audio cassette (analogue)
AC	CD-Audio	Audio compact disc, in CD-Audio or SACD format
AD	DAT	Digital audio tape cassette
AE	Audio disc	Audio disc (excluding CD)
AF	Audio tape	Audio tape (reel tape)
AG	MiniDisc	Sony MiniDisc format
AH	CD-Extra	Audio compact disc with part CD-ROM content
AI	DVD Audio	
AJ	Downloadable audio file	Audio recording downloadable online
AK	Pre-recorded MP3 player	For example, Playaway audiobook and player
AL	Pre-recorded SD card	For example, Audiofy audiobook chip
AZ	Other audio format	Other audio format not specified by AB to AK
BA	Book	Book - detail unspecified
BB	Hardback	Hardback or cased book
BC	Paperback	Paperback or softback book
BD	Loose-leaf	Loose-leaf book
BE	Spiral bound	Spiral, comb or coil bound book
BF	Pamphlet	Pamphlet or brochure, stapled; German ‘geheftet’
BG	Leather / fine binding	
BH	Board book	Child’s book with all pages printed on board
BI	Rag book	Child’s book with all pages printed on textile
BJ	Bath book	Child’s book printed on waterproof material
BK	Novelty book	Use for books whose novelty is expressed in the format itself, not for books in a conventional format which happen to have novelty content
BL	Slide bound	Slide bound book
BM	Big book	Extra-large format for teaching etc; this format and terminology may be specifically UK; required as a top-level differentiator
BN	Part-work (fascículo)	A part-work issued with its own ISBN and intended to be collected and bound into a complete book
BO	Leporello (folded)	A concertina-folded book, usually a picture book
BZ	Other book format	Other book format or binding not specified by BB to BO
CA	Sheet map	Sheet map - detail unspecified
CB	Sheet map, folded	
CC	Sheet map, flat	

Code Value	Code Description	Notes on the meaning and the usage of the code
CD	Sheet map, rolled	See Code List 80 for 'rolled in tube'
CE	Globe	Globe or planisphere
CZ	Other cartographic	Other cartographic format not specified by CB to CE
DA	Digital	Digital or multimedia (detail unspecified)
DB	CD-ROM	
DC	CD-I	CD interactive
DD	DVD	DEPRECATED - use VI for DVD video, AI for DVD audio, DI for DVD-ROM
DE	Game cartridge	
DF	Diskette	AKA 'floppy disc'
DG	Electronic book text	Electronic book text in proprietary or open standard format
DH	Online resource	An electronic database or other resource or service accessible through online networks
DI	DVD-ROM	
DJ	Secure Digital (SD) Memory Card	
DK	Compact Flash Memory Card	
DL	Memory Stick Memory Card	
DM	USB Flash Drive	
DN	Double-sided CD/DVD	Double-sided disc, one side Audio CD/CD-ROM, other side DVD
DZ	Other digital	Other digital or multimedia not specified by DB to DN
FA	Film or transparency	Film or transparency – detail unspecified
FB	Film	Continuous film or filmstrip: DEPRECATED - use FE or FF
FC	Slides	Photographic transparencies mounted for projection
FD	OHP transparencies	Transparencies for overhead projector
FE	Filmstrip	
FF	Film	Continuous movie film as opposed to filmstrip
FZ	Other film or transparency format	Other film or transparency format not specified by FB to FF
MA	Microform	Microform – detail unspecified
MB	Microfiche	
MC	Microfilm	Roll microfilm
MZ	Other microform	Other microform not specified by MB or MC
PA	Miscellaneous print	Miscellaneous printed material – detail unspecified
PB	Address book	
PC	Calendar	
PD	Cards	Cards, flash cards (e.g., for teaching reading)
PE	Copymasters	Copymasters, photocopiable sheets
PF	Diary	
PG	Frieze	
PH	Kit	
PI	Sheet music	
PJ	Postcard book or pack	
PK	Poster	Poster for retail sale – see also XF
PL	Record book	Record book (eg 'birthday book', 'baby book')
PM	Wallet or folder	Wallet or folder (containing loose sheets etc): it is preferable to code the contents and treat 'wallet' as packaging (List 80), but if this is not possible the product as a whole may be coded as a 'wallet'

Code Value	Code Description	Notes on the meaning and the usage of the code
PN	Pictures or photographs	
PO	Wallchart	
PP	Stickers	
PQ	Plate (lámina)	A book-sized (as opposed to poster-sized) sheet, usually in colour or high quality print
PZ	Other printed item	Other printed item not specified by PB to PQ
VA	Video	Video – detail unspecified
VB	Video, VHS, PAL	DEPRECATED - use new VJ
VC	Video, VHS, NTSC	DEPRECATED - use new VJ
VD	Video, Betamax, PAL	DEPRECATED - use new VK
VE	Video, Betamax, NTSC	DEPRECATED - use new VK
VF	Videodisc	e.g., Laserdisc
VG	Video, VHS, SECAM	DEPRECATED - use new VJ
VH	Video, Betamax, SECAM	DEPRECATED - use new VK
VI	DVD video	DVD video: specify TV standard in List 78
VJ	VHS video	VHS videotape: specify TV standard in List 78
VK	Betamax video	Betamax videotape: specify TV standard in List 78
VL	VCD	VideoCD
VM	SVCD	Super VideoCD
VN	HD DVD	High definition DVD disc, HD DVD format
VO	Blu-ray	High definition DVD disc, Sony Blu-ray format
VP	UMD Video	Sony Universal Media disc
VZ	Other video format	Other video format not specified by VB to VP
WW	Mixed media product	A product consisting of two or more items in different media, e.g., book and CD-ROM, book and toy etc.
WX	Multiple copy pack	A product containing multiple copies of one or more items packaged together for retail sale, consisting of either (a) several copies of a single item (e.g., 6 copies of a graded reader), or (b) several copies of each of several items (e.g., 3 copies each of 3 different graded readers), or (c) several copies of one or more single items plus a single copy of one or more related items (e.g., 30 copies of a pupil's textbook plus 1 of teacher's text). NOT TO BE CONFUSED WITH: multi-volume sets, or sets containing a single copy of a number of different items (boxed, slip-cased or otherwise); items with several components of different physical forms (see WW); or packs intended for trade distribution only, where the contents are retailed separately (see XC, XE, XL).
XA	Trade-only material	Trade-only material (unspecified)
XB	Dumpbin – empty	
XC	Dumpbin – filled	Dumpbin with contents
XD	Counterpack – empty	
XE	Counterpack – filled	Counterpack with contents
XF	Poster, promotional	Promotional poster for display, not for sale – see also PK
XG	Shelf strip	
XH	Window piece	Promotional piece for shop window display
XI	Streamer	
XJ	Spinner	
XK	Large book display	Large scale facsimile of book for promotional display
XL	Shrink-wrapped pack	A quantity pack with its own product code, for trade supply

Code Value	Code Description	Notes on the meaning and the usage of the code
		only: the retail items it contains are intended for sale individually – see also WX
XZ	Other point of sale	Other point of sale material not specified by XB to XL
ZA	General merchandise	General merchandise – unspecified
ZB	Doll	
ZC	Soft toy	Soft or plush toy
ZD	Toy	
ZE	Game	Board game, or other game (except computer game: see DE)
ZF	T-shirt	
ZZ	Other merchandize	Other merchandize not specified by ZB to ZF

Appendix E
Encoding Data on the RFID Tag

E.1 Introduction

This Appendix serves as a paper-based tutorial to show the encoding to ISO/IEC 15962 rules in the user memory of an ISO/IEC 18000-3 Mode 1 tag.

The Appendix will not include detailed procedural steps because these can differ between vendors, depending on how they implement the encoding rules of ISO/IEC 15961 and ISO/IEC 15962 (both discussed below). The resultant encoding that is shown in this Appendix is equivalent to compliant encoding, but the detailed processes are not defined. In other words, the document shows what is encoded from different input conditions but not how the encoding process is achieved.

ISO/IEC 15961, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface*, deals with the commands and responses between the application and encoder. This standard was first published in October 2004, and is currently undergoing revisions to be republished as ISO/IEC 15961 Part 1. Although the presentation of commands and responses differs between the two versions of the standards, they essentially provide exactly the same functional requirements.

One major difference between the published version and the revised version of the standard is the removal of some complex transfer encoding rules that were intended to be a formally interface between ISO/IEC 15961 and ISO/IEC 15962. For a number of situations, this proved to be an overly complex conformance requirement.

ISO/IEC 15962, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions*, deals with the process of converting printable characters or those that appear on a screen into a compacted form for encoding on the RFID tag. The encoding rules also provide a way of distinguishing between data elements using object identifiers and, particularly, the Relative-OID as discussed in Section 2.6.

Like ISO/IEC 15961, this standard is also undergoing review and revision. The main feature that impacts RFID for libraries is that the transfer encoding (discussed above) is no longer an input into the encoding procedure. The fundamental encoding rule in ISO/IEC 15962 Rev 1 will remain as defined in the original published version of the standard. New features are being added which might be considered at some future date for the library community, but are probably not relevant for the time being. These include support for other types of RFID tag. With respect to this, the data protocol is intended to support many of the ISO/IEC 18000 series of air interface protocols (i.e., different types of RFID tags) and therefore provides a base for users to adopt additional or different tag types and yet still migrate the data in a compatible manner.

E.2 Assumptions

The detailed illustrative examples in this appendix will make the following assumptions:

- That the memory on the RFID tag is compliant with a monolithic memory structure, where the memory is addressable in a sequence of blocks.
- That the value of the AFI, whether the single value code “C2” is permanently used or the value “C2” is used for on-loan items and “07” is used for in stock items, is unrelated to the encoding example.
- As the AFI is stored in a completely different memory location to the encoded data, that this is also unrelated to the encoding examples.
- The DSFID consists of two components. The assumption is that the access method shall be based on a no-directory structure, where data elements are encoded contiguously one after the other. The second component of the DSFID is the data format, and this has the binary value {xxx00110} as assigned by the Registration Authority of ISO/IEC 15961 Part 2. Combining the value of the access method and data format results in a DSFID value of {00000110}, or “06” as a hexadecimal code.
- The data format provides a method to encode a common Root-OID {1 0 15961 8} once per RFID tag, with only the relative OID being encoded to distinguish between each encoded data elements. Adding the relative OID as a suffix to the root OID creates a unique data element that is distinguishable from all others in the application system.
- As the DSFID is stored in a separate memory on the 18000-3 Mode 1 tag, it forms no part of the encoding examples, other than the fact that all the encoding assumes the correct encoding of the DSFID.
- **All the relative OIDs used in the example are for illustration purposes only.** The formal list of relative OIDs will be specified in ISO 28560.
- Any illustrations for locking of data assume that the tag being used has 4 bytes per block. Users should be aware that ISO/IEC 18000-3 Mode 1 permits the block size to range from 1 byte to 32 bytes. There are RFID tags on the market that have a block size other than 4 bytes, and this will have an impact on the locking of data, both in the encoding rules and across the air interface. In addition, the block size has an impact of reading and writing data across the air interface.

E.3 Compacting the Data

The data is compacted automatically to the rules of ISO/IEC 15962 whenever the ISO/IEC 15961 commands call for the data to be compacted. As different characters can be included in the data, different compaction schemes are called up based on the actual data presented to the data compactor. Data elements may be of variable length, which can result in a significant difference in the number of bytes required to encode the data. The compaction rules defined in ISO/IEC 15962 always call for the most efficient compaction scheme to produce the shortest length of encoded bytes.

The full list of compaction schemes and their codes that are relevant to compacted data is shown in Table 3.

Table 3: ISO/IEC 15962 Compaction Schemes

Code	Name	Description
000	Application-defined	As presented by the application
001	Integer	Integer
010	Numeric	Numeric string (from “0” to “9”)
011	5 bit code	Uppercase alphabetic
100	6 bit code	Uppercase, numeric, etc
101	7 bit code	US ASCII
110	Octet string	Unaltered 8-bit (default = ISO/IEC 8859-1)
111	UTF-8 string	External compaction of ISO/IEC 10646

The compaction scheme is identified by a 3-bit code, as shown in Table 3. The function of the compaction code will be described later.

The application commands of ISO/IEC 15961 include arguments for compaction. If the argument is set to compact the data, then it requires the encoding processes, defined in ISO/IEC 15962, to choose the most efficient compaction scheme ranging from integer to octet string. Sometimes, the length of the user data is relatively short, and compaction cannot be invoked; the data is encoded as “octet-string” with the 3-bit code {110}, enabling direct interpretation when it is read.

If the application command indicates that data is “application-defined” then this instructs the compactor to bypass the compaction scheme and to use the 3-bit code {000} for the encoding on the RFID tag. This ensures that when the tag is read at a subsequent time (sometimes even a different location) that the decoding process carries with it the instruction that the data associated with a particular object identifier is application-defined. A potential use for this is if any data on the tag is to be encrypted. The encryption process could be invoked outside of the scope of the ISO/IEC 15962 encoder (thus preserving some degree of security), and the object identifier clearly defines that the data needs to be decrypted, but only by those who know the rules to apply. Another use is for the OID Index (see Section E.3.9 in this Appendix).

The UTF-8 string is intended primarily for those countries that do not use the ISO Latin Number 1 character set as the basis for their language writing. ISO/IEC 10646 specifies precise rules for UTF-8 encoding, and such encoders are generally available. The intention is for the UTF-8 encoding and decoding to be done externally to the ISO/IEC 15962 encoding rules. The 3-bit code {111} ensures that any reading system is aware that a UTF-8 decode is essential before the data can be correctly displayed on a screen or printed.

Specific examples of encoding particular data elements are described in the following subsections. The reader should note that these examples illustrate the encoding only of the data elements themselves, and that a later section will address encoding of data set, including the precursor, length, and relative OID information.

E.3.1 Primary Item Identifier

The first example for encoding the Primary Item Identifier is based on an all-numeric code, as shown in Table 4.

Table 4: Compacting a Numeric Primary Item Identifier

Data Object	Primary Item Identifier (UII)
Relative OID	1
Data Format	ASCII
Specified Length	Max 16 characters
Example of User Data	12345678901234 Length: 14 digits
Compaction Scheme	001 Integer
Encoded Bytes	0B3A73CE2FF2 Length: 6 bytes

This illustrates the most efficient compaction, because the user data can be converted from a decimal (Base-10) to a binary (Base-2) number. The compaction scheme selected automatically by the encoder is integer with the code {001}.

If, on the other hand, the primary identifier is an alphanumeric code, as shown in Table 5, the compaction will not be as efficient, but will still reduce the number of bytes from the characters presented as user data to the bytes encoded on the RFID tag.

Table 5: Compacting an Alphanumeric Primary Item Identifier

Data Object	Primary Item Identifier (UII)
Relative OID	1
Data Format	ASCII
Specified Length	Max 16 characters
Example of User Data	ABCD123456 Length: 10 characters
Compaction Scheme	100 6-bit code
Encoded Bytes	0420C4C72CF4D768 Length: 8 bytes

In this example, the compaction scheme selected is the 6-bit code {100}, because the characters are a mixture of numeric or uppercase alphabetic.

E.3.2 Owner Library/Institution

The encoding example is based on the International Standard Identifier for Libraries and Related Organizations (ISIL). The following is a description from the ISIL website http://www.bs.dk/isil/structure.htm:

> The ISIL is a variable length identifier. The ISIL consists of a maximum of 16 characters, using digits (Arabic numerals 0 to 9), unmodified letters from the basic Latin alphabet and the special marks solidus (/), hyphen-minus (-) and colon (:). Latin letters modified with one or more diacritics and letters from alphabets other than Latin cannot be used in the ISIL. Each ISIL identifier shall be unique when normalized to the repertoire of characters specified in ISO/IEC-10646-1 without regard to case.

When an ISIL is written, printed, or otherwise visually presented, it shall be preceded by the letters ISIL separated from the identifier by a space. An ISIL is made up by two components: a prefix and a library identifier, in that order, separated by a hyphen-minus. The hyphen-minus is a mandatory character in the ISIL string.

The example of an ISIL code in Table 6 is taken from the ISIL website.

Table 6: Compacting an ISIL Code

Data Object	Owner Library/Institution
Relative OID	3
Data Format	Alphanumeric Per ISO 15511
Specified Length	Max 16 characters
Example of User Data	US-InU-Mu Length: 9 characters
Compaction Scheme	101 7-bit code
Encoded Bytes	AB4D6C9DD556CDEB Length: 8 bytes

The sentence “Each ISIL identifier shall be unique when normalized to the repertoire of characters specified in ISO/IEC 10646-1 without regard to case” has some interesting implications. It means that the ISIL is not case-sensitive, and that examples (as above) that are presented in uppercase and lowercase for eye-readable purposes could be compacted more efficiently. The disadvantage is that the presentation style is lost on decoding. On balance, it is probably better to retain the presentation style of uppercase and lowercase letters and lose the small amount of encoding efficiency.

E.3.3 Set Information

The set information is presented in two components: The ordinal part number followed by the number of parts. If the total number of parts is 9 or less, then the user data can be presented as a 2-digit code. If the total number of parts is between 10 and 99, then the user data is presented as a 4-digit code, as shown in the illustration in Table 7, where the leading zero is an important part of the code structure.

Table 7: Compacting the Set Information

Data Object	Set Info (ordinal part number; number of parts)
Relative OID	4
Data Format	Numeric
Specified Length	2 or 4 digits
Example of User Data	0412 Length: 4 digits
Compaction Scheme	010 numeric
Encoded Bytes	0412 Length: 2 bytes

In this particular encoding example, the leading zero determines that numeric compaction is used, because this preserves the leading zero and returns a 4-digit number on decode. This also ensures that the length of encoding is constant, based on the total number of items in the set. If 9 or less, then encoding is always in a single byte, if 10 or more, the encoding is always in 2 bytes.

E.3.4 Shelf Location

The first example (Table 8) uses a Library of Congress Catalog classification.

Table 8: Compacting the Shelf Location Based on the Library of Congress Catalog Classification

Data Object	Shelf Location
Relative OID	7
Data Format	ASCII
Specified Length	Variable
Example of User Data	QA268.L55 Length: 9 characters
Compaction Scheme	100 6-bit code
Encoded Bytes	441CB6E2E335D6 Length: 7 bytes

To encode all the characters including the period (or full stop) {.}, the 6-bit code compaction scheme is used.

If an in-house system is used containing alphabetic data, it is recommended that this be restricted to uppercase alphabetic characters, as shown in the next example (Table 9).

Table 9: Compacting the Shelf Location Based on a Local Scheme

Data Object	Shelf Location
Relative OID	7
Data Format	ASCII
Specified Length	Variable
Example of User Data	FICTOLKIEN Length: 10 characters
Compaction Scheme	011 5-bit code
Encoded Bytes	324747B1692B80 Length: 7 bytes

Because this scheme only uses uppercase alphabetic characters, the 5-bit compaction scheme is automatically selected. If punctuation or numbers are included in the user data, the most likely result will be that the encoder uses the 6-bit compaction, as in the case of the Library of Congress code above.

E.3.5 GS1 Code

The GS1 code is more popularly understood in the United States as the UCC code, and commonly seen in retail outlets in a bar code format. This includes the encoding of the ISBN, with the prefix '978', and more recently '979'. Since January 2007, the ISBN has formally changed from being a 10-digit code (sometimes with an X check character) into a 13-digit code, as represented in the GS1-13 bar code.

The GS1 code is applied to various other media products, including CDs, DVDs and some periodical publications and some music. There is a scheme for linking the ISSN for serial publications to the GS1 code with the prefix '977'. There is also a scheme that links the ISMN for printed music to the GS1 code with the prefix '979', shared with the ISBN.

The code structure for CDs, DVDs and other products without formal registration code structures follow conventional GS1 rules. This means that for many products that originate in the U.S., the code might need to be expanded with leading zeros to conform to the 13-digit structure. Codes on products from most other countries use the full 13-digit structure. Encoding everything in a 13-digit structure is important because the final digit is a check digit that may be used for validation processes in some systems.

The example illustrated in Table 10 is of a 13-digit ISBN.

Table 10: Compacting the GS1 Code

Data Object	GS1 Code (e.g. ISBN)
Relative OID	10
Data Format	Numeric
Specified Length	13 digits
Example of User Data	9790132837965 Length: 13 digits
Compaction Scheme	001 Integer
Encoded Bytes	08E77163DE4D Length: 6 bytes

Because the ISBN-13 never begins with a leading zero, integer compaction is always applied, and shows a significant level of encoding efficiency. Even for those U.S.-based GS1 codes on CDs and DVDs, compaction will result in encoding of 7 bytes.

E.3.6 Title

The example in Table 11 is typical for a technical reference book. Although the data format is defined as UTF-8, the majority of titles in the United States, including some foreign language titles, will be based on the ISO/IEC 8859-1 Latin 1 character set, which is the default character set for input into the ISO/IEC 15962 encoding procedures.

Table 11: Compacting the Title

Data Object	Title
Relative OID	11
Data Format	UTF-8
Specified Length	Variable
Example of User Data	CJKV Information Processing Length: 27 characters
Compaction Scheme	101 7-bit code
Encoded Bytes	872A5D64127766DFCB6E1E9A77EE414396FC7979F3D3BB3F Length: 24 bytes

The compaction process takes into account the complete character string and, as this example shows, does not achieve a significant reduction in the encoding space required on the RFID tag. The main reason for this is the fact that the user data contains a mixture of uppercase and lowercase letters. In this example, if all the characters had been uppercase, the compaction would have reduced to 21 bytes. Even at this size, encoding a title so that it is easily eye readable consumes a significant amount of memory on the RFID tag.

E.3.7 Order Number

An example of the compaction of an order number is shown in Table 12. One point to bear in mind with respect to the order number is that it can be encoded in the RFID tag as part of the transaction between the book jobber and the library, and then erased. Depending on the extent of preparation for encoding done by the book jobber, a library might be able to overwrite a data element such as the order number with more meaningful data for loan transactions once the book had been received into the system.

Table 12: Compacting the Order Number

Data Object	Order Number
Relative OID	16
Data Format	ASCII
Specified Length	Variable
Example of User Data	AB12345-X Length: 9 characters
Compaction Scheme	100 6-bit code
Encoded Bytes	042C72CF4D6D62 Length: 7 bytes

E.3.8 Supplier Identification

The example in the Table 13 shows the compaction of a supplier identification based on the name of the business.

Table 13: Compaction of the Supplier Identification

Data Object	Supplier Identification Data
Relative OID	18
Data Format	ASCII
Specified Length	Variable
Example of User Data	Book Jobber, Inc. Length: 15 characters
Compaction Scheme	101 7-bit code
Encoded Bytes	85BF7EB412B7E2C59792093BB1FF Length: 14 bytes

This results in a reasonably long user data string, and reasonably poor encoding efficiency. In contrast, if the supplier identification is presented in terms of some code structure, then the user data will be shorter and the possibilities of greater encoding efficiency will exist.

As with the order number, the encoding of the supplier identification might only be meaningful until the item is first registered in the library loan system.

E.3.9 Tag Content Key (Also called OID Index)

The encoding of the OID Index has been left as the last example because the encoding cannot be determined until the other data elements to be encoded have been selected.

Because the encoding is based on a bit string, and this has to be preserved, if ISO/IEC 15961 commands are used, then this data element has to be specified as “user-defined”. If the encoding procedure does not formally use the 15961 commands, but uses some other means of transfer or input, then the functional requirement is that this data element is user-defined and is not to be compacted. More sophisticated encoding systems could have an in-built algorithm that takes the relative OID values for all the selected data elements, and constructs the OID index accordingly. The reader should note that the OID index identifies the relative OID of the encoded data elements in the sequence of the relative OID numbers and not in the sequence in which they appear in the tag memory.

In whatever way the OID index is constructed, care needs to be taken that there is actual encoding capacity for all of the data for the selected data elements. Otherwise, the OID index will indicate that a particular data element is encoded, whereas the actual encoding might fail to achieve what was intended. It follows that the encoding procedure for this particular data element needs to be based on some rigorous procedure to ensure that the OID index is correctly structured to provide its prime function of a very rapid indication of what data is encoded on the RFID tag.

In the example in Table 14, the following three data elements are encoded on the RFID tag:

- Relative-OID 5 ISIL
- Relative-OID 7 Shelf location
- Relative-OID 13 Local Data –1

These three Relative-OIDs {3, 7, 13} require the OID index to have the following bits set to equal 1 {1st, 5th, 11th). This is because the OID index only needs to identify those relative OIDs

that are encoded that are other than the mandatory primary identifier and this conditional OID Index. The basic bit sting of 11-bits needs to be padded with trailing zero bits to align on an 8-bit boundary to create a 16-bit string. This results in a variable length string that may be extended as additional data elements are included, either in the specific library system or added to the data dictionary of ISO 28560.

The bit positions are references to the relative OID, not the sequence of encoding on the RFID tag. For example, shelf location could be encoded before the ISIL and local data, depending on the data capture requirements that are most relevant for the particular library.

Table 14: Encoding of the Tag Content Key (Also called OID Index)

Data Object	Tag Content Key/OID Index
Relative OID	2
Data Format	Bit string
Specified Length	3 bytes
Example of User Data	1000100000100000 Length: 2 bytes
Compaction Scheme	000 User-Defined
Encoded Bytes	8820 Length: 2 bytes

E.4 Data Sets and the Precursor

The ISO/IEC 15962 rules require that the relative OID and compacted data are incorporated into a syntactical structure called a Data Set. There are various rules for data sets, but only two are relevant for the library application: a data set for relative OIDs in the range of 1 to 14, and another for relative OIDs in the range 15 to 127.

E.4.1 The Data Set for Relative OIDs 1 to 14

The structure of an encoded data set for a data element with the relative OID in the range 1 to 14 consists of the following components:

- A Precursor – a single byte that in this case encodes the compaction scheme and the relative OID (the last part of the object identifier)
- The length of the compacted data object
- The compacted data object

This structure is shown in Figure 5. The relative OID values 1 to 14 are directly encoded in the Precursor, and this reduces the amount of memory required for the encoding.

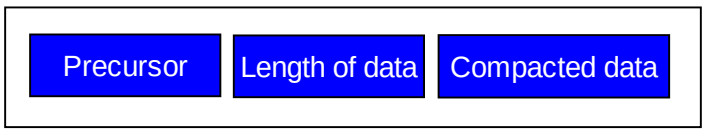

Figure 5: Data Set Structure for Relative-OID Values 1 to 14

E.4.2 The Precursor

For the library applications, the Precursor is a single byte with the bit structure as defined in Table 15.

Table 15: Bit Position of Precursor Components

Precursor Bit Positions							
7	6	5	4	3	2	1	0
Offset	Compaction Code			Object Identifier			

- The **Offset** is associated with the need to align blocks when a data set has to be locked (see this Appendix Section E.5). The offset has the value “0” when no block alignment is applied to the data set, and has the value “1” when block alignment is applied.
- The **Compaction Code** is the 3-bit code as determined by the compaction process.
- The **Object Identifier** is the relative OID, and is the final component of the full object identifier. The value of the relative OID for the primary item identifier number is “1” which encodes as 0001_2. The value of the relative OID for the OID index is “2”, which encodes as 0010_2. If the object identifier is not a relative OID in the range 1 to 14, then the 4-bit code in the precursor has the value 1111_2.

The bit structure of the precursor determines how subsequent bytes in the data set are decoded. The bits that identify the Object Identifier determine whether this is a relative OID in the range 1 to 14, or some higher value. The bits that identify the compaction code ensure that the data is de-compacted using an inverse set of rules to the compaction rules. The offset performs a function (discussed later with respect to locking) that ensures that the sequence of data sets is contiguous.

E.4.3 The Data Set for Relative OIDs 15 to 127

The precursor only provides 4 bits for encoding the object identifier. It is only capable of directly encoding relative OIDs from “1”, which encodes as 0001_2, to “14”, which encodes as 1110_2. For relative OIDs with a value between 15 and 127, of which some are used for the library optional data elements, the last four bits of the Precursor are set = 1111_2. This signals that the relative OID has to be explicitly encoded as a separate component (a single byte) in the data set, as shown in Figure 6.

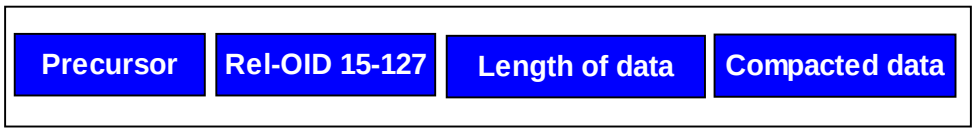

Figure 6: Data Set with Relative OID 15 to 127

The encoded byte value is determined by subtracting 15 from the decimal value of the relative OID, and converting this to a hexadecimal value. For example, relative OID “17” is encoded as “02_{HEX}”.

E.4.4 Encoding the Data Sets

Table 16 shows the structure of the data sets that can result from encoding data elements defined for the library community.

Table 16: Permitted Data Set Structures for Library Data Elements

Description	Structure of Byte String for an Encoded Data Set			
Single Relative OID 1 – 14	Precursor	Length of data	Data ~~	
Single Relative OID 15 – 127	Precursor	Relative-OID	Length of data	Data ~~
~~ Indicates that this component can be multiple bytes. Other data set structures are possible form the encoding rules of ISO/IEC 15962, but these are associated with different object identifier structures, or can apply when data is locked.				

Taking the worked examples in Sections E.3.1 to E.3.9 of this Appendix, it is possible to show the encoding of each individual data set. Because those sections provide alternative examples for the same data element, what follows in Table 17 and Table 18 cannot be seen as encoding on the RFID tag, simply the encoding of individual data sets.

Table 17: The Data Set Examples for Relative OID 1 to 14

Data Element	Example from:	Precursor	Length of Compacted Data	Compacted Data
Primary Item ID	Table 4	11	06	0B3A73CE2FF2
Primary Item ID	Table 5	41	08	0420C4C72CF4D768
ISIL Code	Table 6	53	08	AB4D6C9DD556CDEB
Set Info	Table 7	24	02	0412
Shelf Location	Table 8	47	07	441CB6E2E335D6
Shelf Location	Table 9	37	07	324747B1692B80
GS1 Code	Table 10	19	06	08E77163DE4D
Title	Table 11	5A	18	872A5D64127766DFCB6E1E9A77E E414396FC7979F3D3BB3F
OID Index	Table 14	02	02	8820

Table 18: The Data Set Examples for Relative OID 15 to 127

Data Element	Example from:	Precursor	Relative OID	Length of Compacted Data	Compacted Data
Order No	Table 12	4F	00	07	042C72CF4D6D62
Supplier ID	Table 13	5F	02	0E	85BF7EB412B7E2C597920 93BB1FF

E.5 Locking Data Sets

If the application calls for data to be locked, the encoding rules of ISO/IEC 15962 ensure that this is achieved within the constraints of the ISO/IEC 18000-3 Mode 1 tag. The specification for that air interface protocol allows locking by block, which can be from 1 byte to 32 bytes according to the tag specification, but is commonly—but not always—4 bytes per block. It is essential that any locked data set does not cross over a block boundary and interfere with adjacent unlocked blocks either immediately before or immediately afterwards. Therefore, block alignment is necessary for up to 3 data sets associated with any given locked data set. These are any preceding data set that is unlocked, the data set to be locked, and the unlocked data set that follows.

The problem and solution are illustrated in Figure 7. The illustration on the left-hand side shows three data sets—X, Y and Z—with data set Y requiring to be locked. To lock it, blocks n, n+1, and n+2 would require to be locked, thus corrupting the data sets X and Z because some of the bytes of these blocks would also be locked and therefore it would not be possible to be modified or deleted at some subsequent time. Alternatively, if only block n+1 was locked, then some vital bytes of data set Y would remain unlocked, and therefore subject to change.

By realigning data set Y so that it is block-aligned beginning at block n+1, only this block and block n+2 need to be locked (as shown in the illustration on the right-hand side). There are now some “blank” bytes that need to be addressed. This is done by modifying data sets X and Y as discussed below.

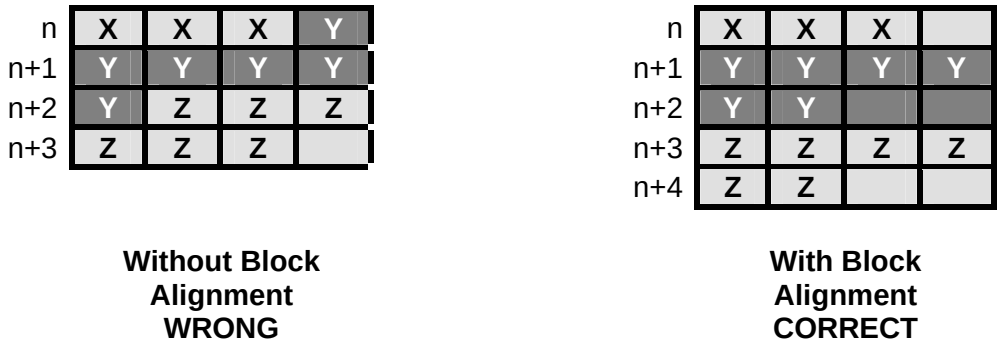

Figure 7: Block Alignment Examples

The data sets need to be encoded in a contiguous sequence, so leaving a gap between data set X and data set Y would result in a failure to properly decode the symbol. The fact that data set X is not locked is immaterial; this alignment is necessary to ensure that data set Y can be read contiguously. The ISO/IEC 15962 rules insert an offset byte immediately following the precursor to begin to achieve this block alignment.

In the case of data set X, the value of the offset byte equals $00_{HEX,}$ indicating that there are no trailing bytes at the end of the data set before the beginning of the next data set. The precursor offset bit is set to 1. On this basis, data set X now completely aligns to the end of a block.

Data set Y requires 2 bytes for block alignment. This is achieved by the offset byte being set to 01_{HEX}, which indicates that an additional byte of a null value (typically 00_{HEX}) follows to achieve block alignment. Again, the offset bit in the precursor is set to =1.

For decoding, if the offset bit in the precursor is set to 1, the decoder knows that an offset byte immediately follows, and that the value of this offset byte determines how many additional null bytes are at the end of the data set before the beginning of the next data set.

In both the examples, without block alignment and with block alignment, data set Z does not occupy all the bytes of its last block. In this particular case, this creates no problems because the data set is unlocked and so the next null byte can be used for encoding an additional data set at a future date. Within the encoding rules, a byte that immediately follows the last data set is defined as the terminator byte and is set to the value 00_{HEX}, which is not a valid precursor at the beginning of a data set.

E.6 Encoding Example

To show the complexities of encoding—all of which are addressed automatically by the encoding rules—the following hypothetical encoding example is described and illustrated in Table 19. This shows that the primary item identifier is encoded in the first position through to the supplier ID being encoded in the last position. At this stage, no block alignment has been undertaken. It should be noted that the OID index identifies the relative OID of the ISIL Code, the Shelf Location, and the Supplier ID in the sequence of the relative OID numbers and not in the sequence in which they appear on the tag.

Table 19: The Data Set Examples for Relative-OID 15 to 127

Data Element	Locked	Precursor	Rela-tive OID	Length of Compacted Data	Compacted Data
Primary Item ID	Yes	11		06	0B3A73CE2FF2
OID Index	No	02		02	8802
Shelf Location	No	47		07	441CB6E2E335D6
ISIL Code	Yes	53		08	AB4D6C9DD556CDEB
Supplier ID	No	5F	02	0E	85BF7EB412B7E2C59792 093BB1FF

The following subsections show a step-by-step encoding of each data set that is achieved through a single process in the encoding rules. The step-by-step approach is used here to show how the encoding builds up and identifies decisions that the encoder has to process.

E.6.1 Encoding the Primary Item Identifier

The precursor, length of compacted data, and the compacted data require 8-bytes. There is also a requirement to lock the data set, but as it is already block aligned it can be encoded in the first two blocks of memory, as shown in Figure 8.

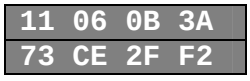

Figure 8: Encoding the Primary Item Identifier

E.6.2 Encoding the OID Index

The data set for the OID index consists of 4 bytes: the precursor, the length of compacted data, and two bytes for the compacted data (Figure 9). This does not have to be locked, because it is encoded in the next block, as illustrated in F5.

11 06 0B 3A
73 CE 2F F2
02 02 88 02

Figure 9: Encoding the OID Index

E.6.3 Encoding the Shelf Location

The data set for the shelf location has 9 bytes, and as this data set is unlocked, could be encoded using 9 bytes. However, looking ahead to the next data set—the ISIL code that requires locking—determines that the shelf location data set needs to be encoded so that it ends block-aligned. As shown in Table 20, the block-aligned data set requires the precursor to have its first bit set to 1, to have an offset byte with the value 02_{HEX}, and to have 2 null bytes encoded at the end of the data. The resultant encoding is shown in Figure 10.

Table 20: Block Aligning the Shelf Location Data Set

	Precursor	Offset	Length	Data	Null Bytes
Pre-alignment	47		07	441CB6E2E335D6	
Block Aligned	C7	02	07	441CB6E2E335D6	0000

11 06 0B 3A
73 CE 2F F2
02 02 88 02
C7 02 07 44
1C B6 E2 E3
35 D6 00 00

Figure 10: Encoding the Block-aligned Shelf Location

E.6.4 Encoding the ISIL Code

The data set for the ISIL code is 10 bytes long. As it requires locking, and the next data set is unlocked, it needs to be block-aligned. This is achieved by inserting the offset byte with the value 01_{HEX} and encoding one null byte value 00_{HEX} following the data. The resultant encoding is shown in Figure 11.

11 06 0B 3A
73 CE 2F F2
02 02 88 02
C7 02 07 44
1C B6 E2 E3
35 D6 00 00
D3 01 08 AB
4D 6C 9D D5
56 CD EB 00

Figure 11: Encoding the Block-aligned and Locked ISIL Code

E.6.5 Encoding the Supplier ID

The data set containing the Supplier ID consists of 17 bytes. As this does not have to be locked, and it is the last data set in the RFID tag memory, no block alignment is required. The encoding is shown in Figure 12.

11 06 0B 3A
73 CE 2F F2
02 02 88 02
C7 02 07 44
1C B6 E2 E3
35 D6 00 00
D3 01 08 AB
4D 6C 9D D5
56 CD EB 00
5F 02 0E 85
BF 7E B4 12
B7 E2 C5 97
92 09 3B B1
FF

Figure 12: Encoding the Supplier Identifier

E.6.6 Selective Reading

On the assumption that the primary item identifier and OID index are of a fixed length for a particular library, the number of bytes required for their encoding can be calculated. Using the example in Figure 9, 12 bytes are all that are required. Using the ISO/IEC 15961 *Read-First-Objects* command, this number of bytes can be entered into the command, account taken of the block size, and the response will deliver (as in the example above) 3 blocks that contain the 12 bytes. If the OID Index is not encoded, then the last block will consist of a sequence of null bytes which the ISO/IEC 15962 decoder will ignore.

Where the system needs to read the shelf location, the same 15961 command can be used, but the number of bytes extended to cover the longest encoding of a shelf location. On the assumption that shelf location coding is as in Figure 10, the interrogator will return 6 blocks of

data and the 15962 decoder will read the primary item identifier, the OID index, and the shelf location data sets.

It is also possible to selectively read an individual data set, by identifying the relative OID necessary to meet the requirements of the application. For example, if there is a requirement to read only the ISIL code, then its relative OID can be specified in a particular command, and that is all that the application would return. The actual implementation in the reader could be achieved in two different ways:

Option 1
The primary item identifier and OID index can be read in the first pass and this would establish that the relative OID for ISIL code is encoded on the tag. The second pass reads from the third block forward with the most efficient air interface implementation being based on some *read until* logic. This requires a stepwise reading of the precursor, any offset, and any length of compacted data, **but skipping over the decode of any data other than the ISIL code**. This process continues until the ISIL relative OID is found, and then the entire data set is either returned or decoded or decoded at the reader.

Option 2
If the library always encodes the ISIL code, then the first stage of reading the primary item identifier and the OID index could be skipped and the reading process begin at the block beyond the OID index. The remainder of the procedure would be as Option 1. This procedure can only be applied if a particular data element is always included on the RFID tag for every loan item in the library. If not, then Option 1 is preferred.

NOTE: This particular procedure might require specific commands to be constructed.

The logic behind selective reading, and particularly the *read until* procedure might require variant implementations. Some RFID tags support the reading and writing of single blocks, others support only reading and writing a contiguous set of blocks, and others support both methods. These are fundamental air interface issues that will affect performance, but are strictly beyond the scope of the ISO/IEC 15962 encoding and decoding procedures. However, the 15962 decoding rules have been built around the fact that not only do different RFID tags support different read commands, but the tags can be completely intermixed in an application and the decoding process still functions normally. As such, the encoding procedure provides a high degree of encoding flexibility, together with support for interoperability of ISO/IEC 18000-3 Mode 1 RFID tags with different memory architectures and command features.

Glossary

AFI	**Application Family Identifier.** A feature of some RFID tags which enables separation of RFID tags by application, so that, for instance, a tag on a library item does not interfere with a system for handling baggage. Also used for security in some library RFID implementations.
EAS	**Electronic Article Surveillance.** The use of electronic systems to secure physical items. Several technologies are included, though the interesting technology used for EAS of relevance to this discussion is implemented using RFID tags.
ILS	**Integrated Library System.** The system that a library uses to manage its collection, typically comprising a database and software to support functions such as circulation, collection management, acquisitions, patron account management, item searching, etc.
NCIP	**NISO Circulation Interchange Protocol.** ANSI/NISO Z39.83-2002. A communication protocol for interoperability among integrated library systems to support library operations: Interlibrary Loan, Direct Consortial Borrowing, and Self Service. The NCIP standard was approved by the National Information Standards Organization in 2002. The intent of this standard is to succeed SIP.
OID	**Object Identifiers.** It is a string of numbers that identifies an object.
RFID	**Radio Frequency Identification.** A technology used for the identification and physical security of items. The technology uses electronic tags for data storage and readers for the reading and programming of the tags.
SIP	**3M™ Standard Interchange Protocol.** A communication protocol that provides a standard interface between a library's integrated library system (ILS) and library automation devices (e.g., check-out devices, check-in devices, etc.). The protocol can be used by any application that has a need to retrieve information from an ILS or process circulation transactions via the ILS. There are two versions of SIP, version 1.0 and 2.0. SIP is based on a proprietary protocol, but has been opened for use by all parties providing systems for library circulation.
UID	**Unique Identifier.** A number or a string of numbers that uniquely identifies an object.

Bibliography

American Library Association. *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles.* Adopted by the ALA Council January 19, 2005. <http://www.ala.org/ala/oif/statementspols/ifresolutions/rfidresolution.htm>

ANSI/NISO Z39.83-2002, *(NISO) Circulation Interchange, Part 1: Protocol (NCIP)*. Baltimore, MD: National Information Standards Organization. <http://www.niso.org/standards/standard_detail.cfm?std_id=728>

ANSI/NISO Z39.83:2002, *Circulation Interchange, Part 2: Protocol Implementation Profile 1*. Baltimore, MD: National Information Standards Organization. <http://www.niso.org/standards/standard_detail.cfm?std_id=805>

DS/INF 163-1:2005, *RFID Data Model for Libraries*. Danish Standards, Charlottenlund, Denmark. <http://www.en.ds.dk/3196>

EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz, version 1.1.0. EPCglobal Inc., December 17, 2005. <http://www.epcglobalinc.org/standards/uhfc1g2>

ISO 15511: 2003, *Information and documentation – International Standard Identifier for Libraries and Related Organizations (ISIL)*. Geneva: International Organization for Standardization. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=27979>

ISO/IEC 10646: 2003, *Information technology – Universal Multiple-Octet Coded Character Set (UCS)*. Geneva: International Organization for Standardization. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39921>

ISO/IEC 15961, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface.* Geneva: International Organization for Standardization. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30528>

ISO/IEC 15962, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions.* Geneva: International Organization for Standardization. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30529>

ISO/IEC 15693, *Identification cards – Contactless integrated circuit cards – Vicinity cards* (in three parts) Geneva: International Organization for Standardization.

ISO/IEC 18000-3, *Information technology – Radio frequency identification for item management – Part 3: Parameters for an air interface communications at 13,56 MHz*. Geneva: International Organization for Standardization. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34114>

ISO/NP 28560, *Information and documentation – Data model for use of radio frequency identifier (RFID) in libraries*. Geneva: International Organization for Standardization. (Standard in development.)

Molnar, D., & Wagner, D. "Privacy and Security in Library RFID: Issues, Practices, and Architectures." 11th *ACM Conference on Computer and Communications Security, October 25-29,* 2004, Washington, D.C. <http://www.cs.berkeley.edu/~dmolnar/library.pdf>

Newitz, A. "The RFID Hacking Underground." *Wired*, 14(5), pp. 166-171, May 2006. <http://www.wired.com/wired/archive/14.05/rfid_pr.html>

ONIX Books Code Lists, Issue 7. EDItEUR, March 2007. <http://www.editeur.org/codelists/ONIX_Code_Lists_Issue_7.pdf>

Rieback, M. R., Crispo, B, & Tanenbaum, A. S. "Is Your Cat Infected with a Computer Virus?" *Proceedings of the 4th Annual IEEE International Conference: Pervasive Computing and Communication*, pp. 169-179, 2006. Washington, D.C.: IEEE Computer Society. <http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/percom/2006/2518/00/2518toc.xml&DOI=10.1109/PERCOM.2006.32>

Rieback, M. R., Crispo, B, & Tanenbaum, A. S. "RFID Malware: Truth vs. Myth." *IEEE Security & Privacy*, 4(4), pp. 70-72, July/August 2006. <http://www.cs.vu.nl/~melanie/rfid_guardian/papers/ieeesp.06.pdf>

Standards Australia Working Group IT-091-01-02. *RFID for Libraries: Proposal for a Library RFID Data Model* (Draft 06), September 2006. <http://www.sybis.com.au/Sybis/4n597-599%20proposal%20document.pdf>