NISO RP-6-2012

RFID in U.S. Libraries

March 2012

A Recommended Practice of the
National Information Standards Organization

Prepared by the
NISO RFID Revision 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This recommended practice may be revised or withdrawn at any time.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

ISBN (13): 978-1-937522-02-5

Table of Contents

Foreword iv

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 and U. S. Profile for ISO 28560-2 5

2.1 Introduction 5
2.1.1 Rationale for the Choice of ISO 28560-2 5
2.1.2 Selection of ISO 28560-2 over ISO 28560-3 6
2.2 Data Objects 6
2.2.1 Advantages of Looking Up Data in the ILS 7
2.2.2 Advantages of Storing Data on the Tag 7
2.3 Mandatory and Optional Data Objects 7
2.4 Locked vs. Unlocked 8
2.4.1 Locking Pros and Cons 8
2.4.1.1 Advantages 8
2.4.1.2 Disadvantages 8
2.5 U.S. Profile for ISO 28560 – RFID in U. S. Libraries 9
2.5.1 Summary 9
2.5.2 Primary Item Identifier 11
2.5.3 Tag Content Key (also called OID Index) 12
2.5.4 Owner Library/Institution 12
2.5.5 Set Information (also called multi-part indicator) 13
2.5.6 Type of Usage 14
2.5.7 Shelf Location 14
2.5.8 ONIX Media Format 15
2.5.9 MARC Media Format 15
2.5.10 Supplier Identifier 15
2.5.11 Order Number 15
2.5.12 ILL Borrowing Institution 16
2.5.13 ILL Borrowing Transaction Number 16
2.5.14 GS1 Identifier 17
2.5.15 Alternative Unique Item Identifier 18
2.5.16 Local Data A 18
2.5.17 Local Data B 18
2.5.18 Title 18
2.5.19 Product Identifier (local) 18
2.5.20 Media Format (other) 19
2.5.21 Supply Chain Stage 19
2.5.22 Supplier Invoice Number 20

2.5.23 Alternate Item Identifier 20
2.5.24 Alternative Owner Institution 20
2.5.25 Subsidiary of an Owner Institution 21
2.5.26 Alternative ILL Borrowing Institution 21
2.5.27 Local Data C 21
2.6 Relative OID 21
2.7 Data Format (DSFID) Declaration 22
2.8 Encoding 22
2.9 Use of Primary IDs and Supply Chain Stages 23

Section 3: Security 24

3.1 RFID Security for Libraries 24
3.2 Application Family Identifier (AFI) 24
3.2.1 AFI Codes and Interoperability 25
3.2.2 AFI Locking 25
3.2.3 Interlibrary Loan Situations 25
3.3 Electronic Article Surveillance (EAS) 25
3.4 Virtual Deactivation (Database Look-Up) 26
3.5 Recommendations for Security 26
3.6 Potential Interference with Non-Library RFID Applications 27

Section 4: Library Migration to ISO Standard Tags 28

4.1 Introduction 28
4.2 Compatibility 29
4.3 Role of RFID Vendor 30
4.4 Role of Integrated Library System Vendor 30
4.5 Suggested Migration Process 30
4.5.1 Migration Considerations 30
4.5.2 On-the-fly Migration 31
4.5.3 Systematic Migration 31
4.6 Questions for RFID Vendors 32

Section 5: The Book Supply Chain: The Value of Standardization 33

5.1 Introduction 33
5.2 Distributors and RFID Tag Applications 33

Section 6: Privacy 36

6.1 Privacy Issues 36
6.2 ALA Resolution on RFID Technology and Privacy 36
6.3 ALA Guidelines on Privacy and Confidentiality in RFID 37
6.4 Implementing the NISO RFID Recommendations and ALA RFID Policy 38

Section 7: Vandalism 39

7.1 Introduction 39
7.2 Modification of Security Data 39
7.3 Modification of Tag Contents 39
7.4 RFID Viruses 39
7.5 Intentional Detuning of the Tag 40
7.6 Physical Defacing or Removal of the Tag 40
7.7 Moving Forward 40

Appendix A: RFID Technology Basics 41

Appendix B: Interoperability Characteristics 47

Appendix C: UHF RFID in Libraries 50

Appendix D: Encoding Data on the RFID Tag 52

Glossary of Acronyms 68

Bibliography 69

Foreword

NISO RFID Revision Working Group Charge

The original NISO RFID Working Group was formed in 2006 to focus on the use and implementation of radio frequency identification (RFID) technologies in U.S. libraries. In January 2008, NISO formally published the Recommended Practice, *RFID in U.S. Libraries* (NISO RP-6-2008). Since that time, 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. After the publication of NISO RP-6-2008, the International Organization for Standardization (ISO) Working Group on RFID in Libraries (ISO TC46/SC4/WG11) produced a three-part standard (ISO 28560) governing the encoding of data on RFID tags for item management in libraries. This work has resulted in ambiguities between the original NISO publication and the final ISO publications. One of the goals of the NISO RFID Revision Working Group is to eliminate these ambiguities.

This revision includes input from RFID hardware manufacturers, solution providers (software and integration), library RFID users, distributors and processors, and related organizations. This revision to the 2008 Recommended Practice was necessary to bring the advice from NISO in line with international standardization efforts. It will also provide United States implementers of RFID tags in libraries sufficient guidance to conform to the ISO work.

Among the goals of this revision and the original document were the following:

- 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.
- To examine and assess privacy concerns associated with the adoption of RFID technologies in libraries.
- 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.
- To focus on security and data models for RFID tags, along with issues of interoperability and privacy.
- To create a set of recommendations for libraries with regard to a tag data model and other issues, with the specific goals for this revision of:
    a. Reviewing and updating information in the original document.
    b. Ensuring conformance between the approved ISO standard and the NISO recommended practice.
    c. Creating a set of recommendations for a U.S. data model standard.
    d. Providing specific examples to make implementation easier for manufacturers and libraries.

Outcomes

The NISO RFID Revision Working Group document recommends a set of practices and procedures to ensure interoperability among U.S. RFID implementations. All sections of the original 2008 document have been reviewed and updated to reflect changes in practices for protection of personal privacy, support advanced functionality, facilitate security, protect against vandalism, and allow the RFID tag to be used in the entire lifecycle of the book and other library materials.

This Recommended Practice includes:

1. A checklist (for libraries and vendors) that can be used to evaluate the degree of conformance with the ISO 28560. This checklist is available at http://biblstandard.dk/rfid/docs/conformance_28560-2.pdf
2. A set of recommend practices and procedures to ensure interoperability among U.S. RFID implementations.
3. A list of suggestions to reduce the impact of migrating from non-conforming systems to conforming systems or running with "mixed" tag systems (older tags and newer conforming tags).

These NISO recommendations for best practices promote procedures that:

a. 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.

b. 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.

c. Protect the personal privacy of individuals while supporting the functions that allow users to reap the benefits of this technology.

d. Permit the extension of these standards and procedures for global interoperability.

e. Remain relevant and functional with evolving technologies.

Early RFID implementers are at considerable risk because of the lack of interoperability of proprietary vendor systems. As RFID providers and libraries adopt tags with the data model recommended in this recommended practice, true interoperability that allows libraries to procure the tags, hardware, and software from independent providers and distributors to use with all tags can become a reality.

The data model outlined in this document is an essential first step. 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:

a. Vendor-specific encrypting and encoding of the data.

b. Proprietary security functions, which are an advantage when considering hackers, thieves, etc., but are a detriment to interoperability (see Section 3).

c. Software or firmware that is system dependent and can only be used with specific tags.

The ideal is that RFID tags compliant with the data model can be usable by other RFID vendors. With standards recommended in this document, interoperability and the ability to embed tags into books at manufacture is within reach.

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)

Eva Bolkovac
Yale University Library

Lettie Conrad
SAGE Publications

Diane Hillmann
Syracuse University

Marjorie Hlava
National Federation of Advanced Information Services (NFAIS)

Rebecca Kennison
Columbia University

Betty Landesman
NIH Library

Rice Majors
University of Colorado at Boulder

Dorothea Salo
University of Wisconsin, Madison

Ken Wells
Innovative Interfaces, Inc.

NISO RFID Revision Working Group Members

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

Livia Bitner
Baker & Taylor

Vinod Chachra (Co-chair)
VTLS, Inc.

Alan Gray
Darien Library

Margaret Hazel
Eugene Public Library

Gretchen Herman
Brodart

Nancy Kress
University of Nevada, Las Vegas

Corrie Marsh
The University of Texas-Pan American

Paul Simon
Checkpoint Systems, Inc.

Paul Sevcik (Co-chair)
3M Library Systems

Rob Walsh
EnvisionWare, Inc.

Daniel Walters
Retired

Trademarks, Service Marks

Wherever used in this recommended practice, all terms that are trademarks or service marks are and remain the property of their respective owners.

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:

a. Reduction of staff manual processes, errors, and repetitive motion
b. Enhanced customer experience through fast and private self check-outs
c. Reduction of staff and patron time spent in finding items
d. Integrated security functionality

While costs continue to decrease due to mass adoption, current RFID implementations require an initial investment and ongoing expense, particularly in the case of a parallel implementation of automated materials handling. While there is a growing body of anecdotal and published reports on return on investment, the rationale for implementation today is usually based on such criteria as:

a. Reduction in the percentage of staff time spent on check-out
b. Reduction in the percentage of staff time spent on check-in
c. Shift in the volume/percentage of check-outs handled by staff versus patrons
d. Increase in circulation handled without additional staff
e. Customer satisfaction with check-out and check-in processes
f. Speed and accuracy of check-in
g. Efficiency of automated materials handling with RFID
h. Speed and accuracy of inventory
i. Consolidation of security functionality eliminating the need for separate magnetic strip or lock boxes
j. Potential for future opportunities to utilize RFID tag data
k. Reduction or avoidance of worker's compensation costs from repetitive strain injuries

1.2 Tagging in Libraries

Libraries typically buy pre-programmed tags or have their distributors 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 a distributor. In the longer term, source tagging at item manufacture is anticipated.

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, with rates of conversion approaching 500 items per hour with two-person teams. Consideration must be given to the cost of buying or renting dedicated stations and their space requirements. Some vendors will quote a per-item price for third party conversion services as an alternative.

1.3 Self Check-Out

Self check-out stations, or kiosks, are generally proprietary touch-screen devices composed of an RFID reader, barcode scanner for library cards, receipt printer, interface software, and, if the library's integrated library system (ILS) does not offer a compatible self check-out module, NCIP (ANSI/NISO Z39.83) or SIP2 protocol software to communicate with the library's ILS application or database. Some vendors configure stations to allow users to view their library accounts, pay fines, and manage their accounts, and nearly all systems provide a basis for staff override in the event of patron difficulty.

It is also possible to procure components or a generic kiosk and outfit it with an RFID reader, barcode scanner, and necessary software inexpensively, 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. Most self check-out systems today use client software on the self check-out unit which communicates with the server software of the ILS, and use the NCIP or SIP2 protocols. There has also been some development of web applications and APIs that may communicate more directly with the ILS.

Self check-out stations allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of items that can be stacked for simultaneous check-outs depends on the read range of the antenna, and the type of items. (DVDs, CDs, and books on CD with their metal substrates reduce the number of items that can be so stacked.) Various means have been developed to try 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 largely counted as successful and while untagged items or patron circumstances—e.g., excessive fines, expired cards, address checks, and other blocks on cards or limits on material types—may still require a staff intervention or check-out, some libraries report seeing self check-out rates range from 30 to 99% of total transactions. Key factors mentioned in high rates of self check-out are intuitive, easy-to-use stations; placement of the self-check stations near to but not immediately adjacent to the staffed circulation desk; 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. Examples of user-friendly loan and fine policies might 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.

Due to concerns regarding decreased read range on metallic content materials, some libraries add various alternative security measures to those materials, which may or may not affect self-check rates. Generic locking cases require staff intervention. Some vendors offer integrated self-check lock boxes that may be automatically unlocked once checked out. The additional cost and usability factors of these measures, or those of a media jukebox, must be evaluated by each library. (For more on security issues, see Section 3.)

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. When check-in takes place manually, RFID also significantly reduces staff repetitive motions.

Conveyor and sorting systems are becoming more prevalent in libraries with the advent of RFID technology. The RFID reader is either mounted in a return chute or over/under a section of a conveyor belt. The item passes over or under an RFID reader—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 for sorting items on hold into specified bins. Systems typically have anywhere from three to fifteen bins or carts, though larger systems utilize a much larger number of bins. It should be understood that RFID return chutes without or with limited sorting capability will require manual intervention to perform accurately, for

example to sort for holds. Their main advantage would be in fast updating of patron records to allow checking out more of a limited collection and the ability to provide check-in receipts automatically.

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. Again, some mechanism for communicating with the ILS, whether it is NCIP, SIP2, web service, or proprietary API, is required to process transactions using data obtained via RFID.

1.5 Inventory Systems

RFID technology can make such routine 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 item 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 any 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 RFID 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. 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. A current benefit of RFID in some ILL processes, even before introducing standardization, 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

Several standards are available to assist with interoperability in the area of RFID in Libraries. These can be divided into two broad categories: Technology Standards and Application Standards. Technology standards define the chips used in the tags and the readers used in RFID, and how they pass information back and forth. Application standards define how the technology is applied to a particular industry—in this case Libraries. The role of the application standards for RFID is to define how data is stored on the chip in the tag. This definition then allows system designers to produce systems that can properly encode and read the tags, even when multiple providers are involved.

There are two International Standards Organization (ISO) / International Electrotechnical Commission (IEC) technology standards pertinent to library RFID tags and readers: ISO/IEC 15693, *Information technology – Radio frequency identification for item management – Unique identification for RF tags*, and ISO/IEC 18000-3, *Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz*, Mode 1. 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. It is important to note, however, that these technology standards view libraries as one niche application in a global industrial landscape. There are many other uses for these RFID standards. Further details on RFID standardization are contained in Appendix A.

When one talks about ISO/IEC standards, it is useful to understand the technical committees and subcommittees, because they have a bearing on how the work gets done and also upon who the stakeholders are. ISO/IEC 15693 is the responsibility of JTC1 (Joint Technical Committee on Information Technology), SC17 (Subcommittee 17, Cards and personal identification). All the ISO/IEC 18000 series standards are the responsibility of JTC1, SC31 (Subcommittee 31, Automatic identification and data capture techniques), WG4 (Working Group 4, Radio frequency identification 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 Application Family Identifier (AFI) (discussed in 3.2) are fundamentally different. Although the same basic chip design 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. The safest position will be to focus on the ISO 18000-3 Mode 1 standard, as this standard is maintained for item management applications.

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. Ultimately, these standards, along with the Danish Data Model (DS/INF 163-1, *RFID-data model*) form the basis for the application standards regarding the encoding of data on tags for the three-part standard ISO 28560, *Information and documentation – RFID in libraries*.

The ISO 28560 application standards are controlled by TC46 (Information and documentation), SC4 (Technical interoperability), WG11 (RFID in Libraries), and are focused on the application of RFID to library needs. ISO 28560-1, *Information and documentation – RFID in libraries – Part 1: Data Elements and general guidelines for implementation*, deals with the definitions of the data elements that may be encoded onto RFID tags in the library application. ISO 28560-2, *Information and documentation – RFID in libraries – Part 2: Encoding based on ISO/IEC 15962*, defines an encoding method for compacting data elements into objects and placing them on RFID tags for use in libraries which utilizes the encoding rules defined in the existing standard, ISO/IEC 15962. ISO 28560-3, *Information and documentation – RFID in libraries – Part 3: Fixed Length Encoding,* defines an encoding method for placing data elements on RFID tags for use in libraries which has its basis in the Danish Data Model.

It is the recommendation of the NISO RFID Revision Working Group that ISO 28560-2 be adopted in the United States for Library RFID Applications. The remainder of this document will provide additional implementation advice based on that recommendation.

Section 2: NISO Data Model and U. S. Profile for ISO 28560-2

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 investments in RFID can be made 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. The specifications contained in the NISO data model provide 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 that 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, Finland, France, and Australia. A few countries in Europe have adopted the Danish model (see http://www.en.ds.dk/3196), in some cases with important variations. Some individual libraries in the U.S. have also adopted the Danish model.

The following sub-sections discuss the choice of ISO 28560-2; the remainder of section 2describes the implementation of ISO 28560-2 for use with RFID in libraries in the United States.

2.1.1 Rationale for the Choice of ISO 28560-2

In late 2007, the initial NISO RFID Working Group published a best practice document (*RFID in U.S. Libraries*, NISO RP-6-2008) recommending data encoding using methods defined in ISO/IEC 15962. Similar approaches were then recommended by the United Kingdom and Australia, and this approach has been standardized on a global basis in ISO 28560-2, with data elements defined in ISO 28560-1. Simultaneously, the Danish model has been adapted to create ISO 28560-3, again with data elements defined in ISO 28560-1.

When the NISO RFID Revision Working Group began its chartered discussions in 2010, it considered whether to recommend adoption of all parts of the ISO 28560 family for use in the U.S., or whether to recommend a single encoding method. The following impacts of this decision were considered:

- Interoperability – Despite advances by RFID providers in the management of collections using multiple RFID tag data formats, and seeing future requirements for interlibrary borrowing, the need for interoperability is best served by recommendation of a single standardized format for the U.S.
- Ambiguity – Forcing individual library systems to select one of two recommended formats was viewed as an unnecessary burden. An implicit part of the working group's charge was to provide an informed recommendation for libraries wishing to invest in the benefits of RFID technology. To abdicate this responsibility would limit the benefits of the technology and would make it less accessible to the library community.
- Legacy – Some portion of the libraries in the U.S. have already adopted the Danish data model. Many others are using proprietary models. To truly comply with either of the ISO encoding methods requires some reprogramming of the tags for any of these libraries. Thus the decision to recommend one and only one of the ISO encoding schemes does not represent an unnecessary burden to particular libraries based on previous choices–all tags require some reprogramming to comply.

After discussion it is the considered collective opinion of the NISO RFID Revision Working Group that the interests of U.S. Libraries are best served by standardizing on just one of these encoding methods for use

in the U.S. and, **as indicated previously, the Working Group recommends the ISO 28560-2 method, based on ISO/IEC 15962**.

2.1.2 Selection of ISO 28560-2 over ISO 28560-3

The choice of ISO 28560-2 over ISO 28560-3 was made after considerable deliberation and is based on the following factors:

- Efficiency – The ISO 28560-2 support of variable length encoding generally requires less memory space on the tag for equivalent tag content, compared with ISO 28560-3. The tag content key field immediately informs the software of all the data that exists on the tag. This can improve system performance by decreasing the size of data that is read from and written to the tag (though it does require the RFID system to manage the fact that the precise location of a data element on the tag is not predetermined). Avoiding unnecessary reads to the tag. will ultimately lead to faster material handling
- Flexibility –The ability to pick and choose the fields that will be encoded on an RFID tag and ignore the rest (barring the two mandatory fields) is important to U.S. libraries. This flexibility allows different libraries to use different parts of the data model and yet be consistent with the U.S. profile for ISO 28560-2. Different regions of the country or different types of libraries can have their own profiles (sub-profiles of the U.S. profile) to better serve the needs of their communities. The implementation of ISO 28560-3 in the U.S. makes sense only if there is a requirement for backward compatibility with the Danish model.
- Security – Locking of data, if desired by the library, can be selected for individual data elements in ISO 28560-2, where the entire basic block must be locked in ISO 28560-3, if locking is to be employed.
- Future compatibility – Future changes to the standards, through the addition of new data elements, is more streamlined in ISO 28560-2 and does not rely on version numbering, which can be complicated in ISO 28560-3 by the above constraint on locking. (Note that addition of new data elements must be undertaken by ISO.)

This direction is consistent with the approach recommended by the first NISO RFID Working Group and the RFID Revision Working Group concurs with the choice of ISO 28560-2 encoding over backward compatibility with the Danish model.

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 chip 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 it will bring to the application. Third, it is important to keep the read time of the tag as short as possible. In some cases, more than one read may be required to retrieve all the necessary data from the tag. All of these issues 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.

In the development of a U.S. Profile for compliance with ISO 28560, the NISO RFID Revision Working Group considered the merits of several data elements, and resisted the exclusion of elements that were considered potentially useful in the future. Some of these data elements have generated privacy or other

concerns in the past, and the working group felt that while libraries should consider those concerns when making decisions about the use of the data elements, these should not be specifically excluded since their acceptability or utility may change over time.

The recommendations for this U.S. data model include the addition of the owner library identifier in combination with the primary item identifier to create a nationally unique item identifier. Additional data elements are optional, or in a few cases excluded. While not adhering to the absolute minimalist approach, this gives the library flexibility to have a smaller or larger data set based on individual local requirements.

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, storage of data on the tag adds the cumbersome requirement of having the physical item in hand to make an update. So libraries are cautioned against this practice, although sometimes there are good reasons for employing it.

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. Keeping the size of data on the tags relatively small allows manufacturers the opportunity of producing tags with less memory, thereby reducing the tag costs to the library.

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 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 for 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. Upstream from the library, suppliers or publishers may add data to be used by a receiving library, but not particularly by the ILS. Individual library practice may also require adding information not defined by the recommended model. The data model allows for this usage by defining three data objects, Local Data A, Local Data B, and Local Data C (see Section 2.5).

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

- The minimum amount of data to support the RFID system at a national level. In the data model below, this category includes both the Primary Item Identifier and the Tag Content Key.
- Data on the tag that enhance the operation—for example, data from suppliers that can assist with receiving functions, or data indicating that the item is part of a set and that other items are necessary to complete the transaction.
- 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

The practical application of the ISO 28560 family of standards for *RFID in Libraries* demands not only that a country ideally settle on one encoding method for best interoperability, but also that a profile be defined that identifies which data elements are mandatory or optional, which data elements should be locked, and any data elements which should not be encoded. The subparts of this section comprise the U.S. profile for ISO 28560.

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 so that systems can be designed counting on their presence. In some cases, an element is only mandatory if the library uses that particular identifier, e.g. an ISIL code. These elements are marked "Mandatory if applicable."

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 community 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". Additionally, where the ISO 28560 family defines a data element that this document is recommending as not to be encoded in the U.S., that data element is designated as "excluded".

2.4 Locked vs. Unlocked

Most modern tags with read and write capability also offer the ability to write data onto 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 non-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.

2.4.1 Locking Pros and Cons

Locking data on RFID tags offers advantages and disadvantages to a library, so a considered approach is warranted. This section will discuss some of the most apparent benefits and disadvantages of tag data locking:

2.4.1.1 Advantages

a. Locking protects the locked data from inadvertent or intentional modification by an entity with an RFID reader.

   Consideration should be given to the potential for local staff or a borrowing library to inadvertently modify tag contents. Also as RFID readers become more common in devices carried by the general public, such as smartphones, there is the potential for inadvertent or intentional modification of tag contents. It is important to note that neither of these possibilities has manifested itself in any significant way in libraries to date, and RFID readers have been available to technically savvy individuals for years at fairly low cost. As they move into smartphones, however, the potential for misuse of the devices in a library increases.

2.4.1.2 Disadvantages

a. Locking typically introduces some additional time and complexity in the tag programming process.

   Before a library or service provider commits to locking data on a tag, it will want to be very certain that the data is correctly programmed. Even if these checks can be done completely automatically, they may involve additional read operations on the tag, which takes a small amount of time. If the checks must be done by staff, there is more potential for error, the training requirements are increased, and the overall processing time may be significantly increased. Service providers may pass this burden on to the library in the form of increased costs for the service provided.

b. Locking prevents a library from modifying the locked content of a tag when it may be convenient to make a modification.

Examples of instances where a library may want to make modifications to a tag include changes to primary item identifier or owning library identifier, or circulation status (if stored on the tag). If any of these data elements are locked and the library wishes to change them, the tag will likely require replacement. Library policy or procedures can be used to minimize the impact of these factors by either limiting the locked data to only particular data elements or by finding procedural alternatives to changing the data. For example, if the need to change an item identifier is based on the need to replace a damaged optical barcode label, the barcode label could be duplicated rather than adopting a new item identifier number from a new label.

c. If the data is locked, the tag cannot be reprogrammed to conform to a new tag data standard.

   This disadvantage is one often cited for proprietary or vendor-defined tag data formats. Despite significant efforts by the developing organizations, there is always the finite possibility that a standard will not perform well technically, or for other reasons it may not be well accepted and then the library will wish to reprogram to a different format in the future.

d. The flexibility of encoding tags according to ISO 28560 brings a complication when locking of data is considered.

   If a library or system implementer chooses to lock data in particular blocks of the tag such that there might be unlocked data surrounding the locked areas, the process of modifying tag contents becomes more challenging, as the system must steer the data elements around the locked data, which is an obstacle in this case.

2.5 U.S. Profile for ISO 28560 – RFID in U. S. Libraries

2.5.1 Summary

The model specifies a total of 26 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. This is consistent with the data elements and the encoding specified in ISO 28560-1 and ISO 28560-2. Table 1 below contains six columns. Together they represent the *U.S. Profile for ISO 28560 – RFID in U. S. Libraries*.

Table 1: U.S. Profile for ISO 28560 – RFID in U. S. Libraries

Data Object	Relative OID*	Formatting	Category	Main Purpose or Codes Used	Locked If Used?
Primary Item Identifier (unique item identifier)	01	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Mandatory	Item identification	Optional
Tag Content Key (also called OID Index)	02	Bit mapped code	Mandatory	Determining what other data is on the tag	No
Owner Library/Institution	03	Variable length. Max: 16 bytes	Mandatory if applicable	Identification – use ISIL code (ISO 15511)	Optional
Set Information (also called multi-part indicator)	04	{Total in Set / Part Number} structure. Max: 255 bytes	Optional	Item properties	Optional
Type of Usage	05	Fixed length. 1 byte	Optional	Item usage (coded list)	Optional

Data Object	Relative OID*	Formatting	Category	Main Purpose or Codes Used	Locked If Used?
Shelf Location	06	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	Support inventory – (LC Call Number, Dewey)	Optional
ONIX Media Format	07	Fixed length. 2 uppercase chars.	Optional	Item properties (ONIX code list)	Optional
MARC Media Format	08	Fixed length. 2 lowercase chars.	Excluded	Item properties (MARC code list)	N/A
Supplier Identifier	09	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	Acquisitions processing	Not recom-mended
Order Number	10	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	Acquisitions processing	Not recom-mended
ILL Borrowing Institution	11	Variable length. Max: 16 bytes	Optional	Support ILL – use ISIL code (ISO 15511)	No
ILL Borrowing Transaction Number	12	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	ILL transaction tracking	No
GS1 Identifier	13	Fixed length. Numeric field. 13 digits.	Optional	Identification	Optional
Alternative Unique Item Identifier (reserved)	14	Variable length.	Optional Should not be used until defined by ISO 28560.	Identification	Not recom-mended
Local Data A	15	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV, or UTF-8	Optional	For local or regional use	Optional
Local Data B	16	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV, or UTF-8	Optional	For local or regional use	Optional
Title	17	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV, or UTF-8	Optional	Identification	Optional

Data Object	Relative OID*	Formatting	Category	Main Purpose or Codes Used	Locked If Used?
Product Identifier (local)	18	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	Identification	Optional
Media Format (other)	19	Single octet (coded list).	Optional	Item properties (no code list defined)	Optional
Supply Chain Stage	20	Fixed. 1 byte	Optional	For multi-use (coded list)	No
Supplier Invoice Number	21	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Excluded	Acquisitions	N/A
Alternative Item Identifier	22	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	Item identification	Optional
Alternative Owner Institution	23	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Mandatory if applicable	Item identification for codes not ISIL compliant	Optional
Subsidiary of an Owner Institution	24	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	Item identification	Optional
Alternative ILL Borrowing Institution	25	Variable length. Alphanumeric. Character set = ISO/IEC 646 IRV	Optional	Support ILL – for non-ISIL code	No
Local Data C	26	Variable length Alphanumeric. Character set = ISO/IEC 646 IRV, or UTF-8	Optional	For local or regional use	Optional
*See Section 2.6.					

2.5.2 Primary Item Identifier

Note: This element is referred to as Primary Item ID in this recommended practice, which reflects how it is commonly used in the U.S.

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. (See also Section 5.)

To create an identifier that is nationally and potentially globally unique, the Primary Item ID can be used in combination with the Owner Library/Institution data element (see 2.5.4).

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Mandatory	Variable length supporting full ASCII (ISO/IEC 646 IRV) character set (Expected length 16 bytes, but not limited in ISO 28560-2.)	Optionally locked when used in library; unlocked in upstream supply chain	In ISO 28560-2, this data element must be physically the first data element in the tag memory.

2.5.3 Tag Content Key (also called OID Index)

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 26 data objects and two of them are not represented in the key, only 24 bits are needed to flag the 24 additional data objects. It is necessary to maintain byte boundaries in encoding the data. Since there are exactly 24 additional data objects, only three bytes are needed. Note that if the data elements populated comprise only lower-numbered OIDs, it is not necessary to program the Tag Content Key to its full potential length.

EXAMPLE:

Assume that the tag has two additional data elements encoded on it. Further assume that the two elements are owner library/institution and GS1 product identifier. According to the model, these are the first and the 11th additional elements. Thus, the content key will be coded with 1 in the first and 11th position and zeroes elsewhere. The encoding therefore will be:

Code: 1000000000100000

Position: 1234567890123456
(showing 16 bits in use)

If no additional data 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, and this can be represented either as coded zeroes or as a truncated string. There is one other very important implementation detail presented below.

The mandatory nature of this data object is linked to the presence of additional data items on the tag. It allows a quick determination of which other fields are populated on the tag.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Mandatory (to comply with the profile, additional data is encoded)	Variable length – dependent on the encoded data set on the tag	Unlocked	Must be encoded directly after the Primary Item Identifier in the physical tag memory

2.5.4 Owner Library/Institution

This element is used to identify the owning library or other institution using an ISIL-compatible code. 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.

The combination of Owner Library/Institution and Primary Item ID can also form a globally unique identifier for an item.

The ISIL is useful enough on a global basis that a library that does not have an ISIL compatible code should consider obtaining one before undertaking an RFID tagging project. If this is not possible, or is otherwise not desired, then a non-ISIL code may be encoded in the Alternative Owner Library data element. If the library has an ISIL, this element is required.

The ISIL Code is defined in ISO 15511, *Information and documentation – International Standard Identifier for Libraries and Related Organizations (ISIL)*. Part 1 of ISO 28560 clearly specifies that for interoperability purposes the ISIL code be used. This recommendation is carried forward in this Recommended Practice. More information about the structure of the ISIL code may be found at the Registration Authority for ISIL website: http://biblstandard.dk/isil/structure.htm.)

The reader should note that some commonly used library identifier codes are ISIL-compatible, including OCLC codes. (See http://biblstandard.dk/isil/index.htm.)

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Mandatory if applicable (i.e. if the organization has an ISIL-compatible code) Either this data element ***or*** the Alternate Owner Institution data element must be populated.	Variable length not to exceed 16 bytes with formatting as specified above	Optional to lock if used	Encoded according special rules included in ISO 28560-2

2.5.5 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 any multi-part item are circulated as a single unit.

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 total number of parts followed by the ordinal part number. 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, with the lowest ordinal values shown as 00 to 09. If the total number of parts is between 100 and 255, then the user data is presented as a 6-digit code. In this case, if the ordinal value is less than 100, it is prefixed by leading zeros to create a 3-digit number. (See Section D.3 in Appendix D.)

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional (but Mandatory for multi-part items when RFID is used to assist with the management of the parts)	Variable length of one, two, or three bytes	Optional lock if used	N/A

2.5.6 Type of Usage

This data object provides information about the intended use of the item, e.g., whether circulating or reference only. For circulation purposes, the values can specify whether the item is allowed to circulate according to normal policies, or whether, in some cases, the item should receive special treatment, such as in an automated material handling systems. A full table of values can be found in ISO 28560-1.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Fixed length of 1 byte	Unlocked	N/A

2.5.7 Shelf Location

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

a. By Library of Congress (LC) call number

b. By Dewey Decimal classification

c. 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 specify its shelving method. Automatic sorting systems sometimes use a 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:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Unlocked if used	N/A

2.5.8 ONIX Media Format

This data object is used to specify the format of the media being circulated.

The NISO RFID Working Group recommends utilizing the media format codes from the *ONIX for Books Code List* produced by EDItEUR, which is widely supported by BISG (Book Industry Study Group) in the United States. These codes are included in List 7 of the Code List and referred to as Product Form Codes[1]. ISO 28560-1 recommends use of the most current list.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Fixed length of 2 bytes	Optional lock if used	N/A

2.5.9 MARC Media Format

This data object is used to specify the format of the media being circulated.

It is the inclination of the NISO RFID Working Group to adopt the ONIX coding scheme for media format (see 2.5.8), which is widely supported by BISG (Book Industry Study Group) in the United States. The MARC Media Format data element is excluded from use in the U.S.

Properties: Excluded

2.5.10 Supplier Identifier

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 (ANSI/NISO Z39.43)). Its definition is to be agreed between the supplier and the library.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Locking not recommended	N/A

2.5.11 Order Number

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

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable Length	Unlocked if used	N/A

[1] EDItEUR. *ONIX for Books Code Lists*. Available from: http://www.editeur.org/14/Code-Lists/
Note: List 7, Product form code, and List 150, Product form, have 111 codes in common. List 7 has 10 codes not included in List 150 and List 150 has 13 codes not included in List 7. According to EDItEUR, List 7 should suffice for RFID applications and it is the list recommended by the ISO 28560 Standard.

2.5.12 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 library/institution described in Section 2.5.4, except that this data object is always unlocked.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length not to exceed 16 bytes with formatting, as specified in 2.5.4 above	Unlocked if used	Encoded according to special rules defined in ISO 28560-2

2.5.13 ILL Borrowing Transaction Number

In addition to the ILL Borrowing Institution data element (see 2.5.13), there is an additional data element that will facilitate the tracking of ILL transactions. In interlibrary loan transactions in the U.S., the process generally has the following steps:

a. 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.

b. 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.

c. The ILL management software initiates contact with the first candidate lending institution, requesting a loan of the item, identified bibliographically.

d. 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.

e. 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.

f. When the borrowing library receives the item, it generally creates a temporary record in 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.

g. 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.

h. 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 Borrowing Transaction Number, 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 Borrowing Transaction Number 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:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length – expected to be 9 digits	Unlocked if used	N/A

2.5.14 GS1 Identifier

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

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 product identifier data element shall, if encoded, be used to store the GTIN-13 code of GS1.

The Global Trade Item Number (GTIN) is a code that identifies the product – not the individual item.

The GTIN-13 has 13 digits and is commonly seen on retail products in a barcode format and is (without the check digit) also an element of tags used in retail that follow the electronic product code scheme of GS1 / EPC Global. The GTIN-13 code is commonly called the UPC code in the United States, and in other parts of the world it is known as the EAN-13 code).

The GTIN–13 code includes the encoding of:

- the ISBN, with the prefixes '978' and '979';
- the ISSN with the prefix '977'; or
- the ISMN with the prefix '979'.

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 D.3.5 of Appendix D).

Since the GS1 code does identify the specific material to which the tag is attached, its existence on the tag while the item is circulating represents a possible privacy risk. Libraries are encouraged to consider the risks and benefits of populating this data element at different points in the lifecycle of the item when determining whether to use the data element, and whether to lock it in tag memory.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length – expected to be 13 digits	Locking optional	N/A

2.5.15 Alternative Unique Item Identifier

The Alternative Unique Item Identifier is a reserved field awaiting definition in a future release of ISO 28560. While it is shown as optional, it shall be used only after it is defined by revisions to the ISO 28560 family.

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Locking not recommended	N/A

2.5.16 Local Data A

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:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Locking optional	N/A

2.5.17 Local Data B

A second data object, similar to Local Data A.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Locking optional	N/A

2.5.18 Title

This element is the title of the library item.

Since the Title does identify the material to which the tag is attached, its existence on the tag while the item is circulating represents a possible privacy risk. Libraries are encouraged to consider the risks and benefits of populating this data element at different points in the lifecycle of the item when determining whether to use the data element, and whether to lock it in tag memory.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length – no maximum length specified, though the expected length is 32 bytes	Locking optional	N/A

2.5.19 Product Identifier (local)

This element is the identifier of a product not linked to the individual item and not based on the GS1 codes.

This other product identifier data element may be used for items that do not have a GS1 code or for which the GS1 code is not known or not adequate. This enables information systems linked to various code structures to be supported by the RFID system.

Since the Product Identifier does identify the specific material to which the tag is attached, its existence on the tag while the item is circulating represents a possible privacy risk. Libraries are encouraged to consider the risks and benefits of populating this data element at different points in the lifecycle of the item when determining whether to use the data element, and whether to lock it in tag memory.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Locking optional	N/A

2.5.20 Media Format (other)

This data object is used to specify the format of the media being circulated.

The NISO RFID Working Group recommends utilizing the media format codes from the *ONIX for Books Code List,* produced by EDItEUR, in the ONIX Media Format element (see 2.5.8). However, Media Format (other) is also part of the ISO 28560 standard, to be used for any coding other than ONIX or MARC.

If Media Format (other) is used, the data element coding is defined locally by the system.

Should a library elect to utilize Media Format (other), it is important that its definition be consistent with any other Media Format data elements encoded on the tag, such as the ONIX data element. Population of multiple media format data elements is not recommended, as they must not conflict with each other, and this may be a difficult task.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Fixed length of 1 byte	Locking optional	N/A

2.5.21 Supply Chain Stage

As explained in Section 5, the NISO RFID Working Group expects that RFID tags will 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. However, 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 they 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 – RFID in* ***Libraries*** (ISO 28560) [bold emphasis added].

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 has included the “Supply Chain Stage” data object on the tag to allow different data to exist on the same tag at different stages in the lifecycle, 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 address the needs of international library communities and yet keep the door open for any communications and negotiations with other members of the U.S. supply chain.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Fixed length of 1 byte with values shown above (Other values may be added later but must be specified by NISO.)	Unlocked if used	N/A

2.5.22 Supplier Invoice Number

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

Properties: Excluded

2.5.23 Alternate Item Identifier

The Alternate Item Identifier (not necessarily a unique ID) is assigned when parties involved with an item deem it necessary to have an item identifier which cannot be accommodated by the Primary Item ID. An example may be during the acquisition process, when the element might be used by the supplier and library to identify the material being delivered to the library. It should not be the ISBN, as this would be coded in the GS1 product identifier field. In this example, this number has application (or meaning) only to the supplier and is used to return items to the supplier.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length – alphanumeric data with expected length of 16 bytes	Locking optional	N/A

2.5.24 Alternative Owner Institution

This element is required to identify the owning institution **in the event that an ISIL compliant identifier is not available**. When necessary, it should be used instead of the Owner Library/Institution Identifier data element; it is not to be used in addition to that data element.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Mandatory if applicable (i.e. if the library has no ISIL code) Either this data element ***or*** the Owner Library Institution data element must be populated.	Variable length	Locking optional If a library anticipates a future assignment of an ISIL code, it may be beneficial to leave this data element unlocked.	N/A

2.5.25 Subsidiary of an Owner Institution

This element is used to identify ownership by a particular subsidiary or branch of the owning institution of the item. When necessary, it should be used in addition to the Owner Institution data element or the Alternative Owner Institution; it is not to be used independently from one of those data elements.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Locking optional	N/A

2.5.26 Alternative ILL Borrowing Institution

This element is used to identify the borrowing institution in an ILL transaction, in the event that an ISIL compliant identifier is not available.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Unlocked if used	N/A

2.5.27 Local Data C

A third data object, similar to Local Data A.

Properties:

Requirement	Fixed or Variable	Locked?	Encoding
Optional	Variable length	Unlocked if used	N/A

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 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.
>
> 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).[2]

The use of relative object identifiers in the range from 15-127 requires an additional byte of overhead in the data element, so typically these OID values are used on data elements which are expected to be encoded less frequently.

This object identifier structure involves the use of Application Family Identifier (AFI) and Data Storage Format Identifier (DSFID) codes programmed into the tags. Think of the AFI and DSFID codes as providing the street address in the above example, with the relative OID providing the apartment number.

The OID assignments utilized in this document are governed by ISO 28560-2.

2.7 Data Format (DSFID) Declaration

The data storage format identifier (DSFID) value 6 (xxx00110b) has been assigned by ISO for library use when a tag is encoded according to ISO 28560-2. In addition to declaring that the tag conforms to ISO 28560-2 encoding, this value also confirms the access method. See ISO 28560-2 for additional information.

2.8 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 15962 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 6-7 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, ISO/IEC 8859-1, and UTF-8, which should cover most all

[2] Standards Australia Working Group IT-091-01-02. *RFID for Libraries: Proposal for a Library RFID Data Model (Draft 06)*. Nunawading, VI: Sybis, September 2006, pp. 10-11. Available from: http://www.sybis.com.au/Sybis/4n597-599%20proposal%20document.pdf

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 D shows details on the encoding scheme standardized in ISO 28560-2.

2.9 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. This data is essential for the RFID applications to work correctly.
- Primary Item ID data object in stages of the supply chain other than the library 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, the link between the UID and Primary Item ID is possible in the library stage. 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 may be *locked*. In library settings where items are made accessible to the public, the Primary Item ID field may be locked as an additional precaution against vandalism or accidental alteration or erasure. See section 2.4.1 for additional details.
- 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 may become 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.

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;
- multiple item sets where the tags are placed very close to one another (and the security marker may not be set properly on each item in the set at check out);
- material of which the items are made;
- DVDs, CDs, and other items with metallic content in close proximity to the RFID tags;
- size of the RFID tags;
- tuning of the antennas on the hardware that interacts with the RFID tags;
- electro-magnetic interference caused by nearby devices and equipment;
- orientation of the tags in the portal; and
- whether the system supports 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 Application Family Identifier (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 tag 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 the two AFI codes authorized by ISO for use by libraries for library items. This facilitates interoperability with other applications.

As defined in ISO 28560-1, 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 $(07)_{HEX}$ 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; the AFI code or EAS bit will be seamlessly reprogrammed 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, but in any event, the owning library should not have the burden of any reformatting of the data elements altered by the borrowing 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 simple 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.

In the context of library item security, the gates positioned just inside the exit act as the interrogators. If they detect any tags whose EAS bit is set to "on," they generate 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 status of each checked out item. 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 as 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 to coexist that use different methods to process security information 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.

3.6 Potential Interference with Non-Library RFID Applications

As RFID use continues to proliferate both within and outside the library industry, the potential for interference with other systems also grows. Consider for example a library patron who has just left a local bookstore where she purchased a new book. If the bookstore and the library both use RFID for stock management and security, how can we ensure that books purchased from the bookstore do not activate the library's security gates? Likewise, how do we prevent library items from alarming at the bookstore?

While it may not be possible to completely eliminate these kinds of interferences, there is functionality that may help to reduce the potential for them to occur.

- Most retail and pharmaceutical uses of RFID utilize UHF tags, while HF tags are more common in libraries. These two tag types require different readers so interference is not likely.
- Library applications should use the appropriate AFI byte values with their tags, and they should ignore tags with different AFI byte values. By alarming only on the specific AFI assigned to items that are considered checked-in, library applications should be able to remain oblivious to RFID tags from other industries.

Section 4: Library Migration to ISO Standard Tags

4.1 Introduction

Libraries with existing RFID installations are unlikely to be compliant with all the data requirements of the new standard. While most tags purchased today and in recent years are in compliance with ISO 18000-3 Mode 1, vendors have historically used proprietary approaches to encoding data on the tags. In other words, even if two installations use ISO 18000-3 Mode 1-compatible tags and readers, they may not be able to interoperate since the data at each respective site may be encoded differently. Think about going to a bookstore and selecting a book in a language you cannot read. While you may be able to recognize the letters and see words and paragraphs, you cannot decipher the actual meaning of the text. Defining a standard data model for encoding is the problem that ISO 28560 intends to address. The question now is whether a site with existing tags and equipment can successfully migrate to an ISO 28560 compliant solution. Theoretically, if a library uses ISO 18000-3 Mode 1-compliant tags, readers, and other hardware, such a migration may be possible. However, issues like whether the data on the existing tags are locked and what sort of model is in place for security will affect migration. 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 and existing components, the labor and disruption involved can be minimized. Over time, thanks to a uniform standard, libraries will be able to operate with equipment from multiple vendors and suppliers.

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, this kind of library-to-library interoperability can be achieved.
- Supply stream interoperability – A standard data model will make it much less expensive for distributors who offer pre-processing and will be an easier option for publishers and other supply stream elements to consider.
- 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, all implementers should make sure that they are ISO compliant and using an officially assigned AFI code. The codes are referred to in Section 3.2.
- Equipment replacement – This is the other benefit of interoperability. Libraries are concerned about the future value of their investments and they are resistant to the concept of being locked to a particular vendor based on past choices. By migrating tag data formats to a standard, when equipment upgrades and expansions are considered in the future, 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. Other sections of this document describe 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 effort for a migration to any new data model, such as the one described here. There will be work involved in equipment upgrades and staff time will be consumed where personnel are employed to reprogram tags, as well. The labor required for a migration can be minimized through thoughtful planning and many vendors offer services to assist with this process.
- 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. How this cost is absorbed by the industry will probably vary from vendor to vendor and library to library.

Most standards activities undertaken today on a global basis are suggesting that these RFID tags are a good choice for interoperability. If the systems used to program the tags for use in the library have anticipated 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:

- In the past, most offered tags were proprietary, which presents scenarios in which tags cannot be reprogrammed. Compliance with the recommended model in this document should ensure the use of the tags over the lifetime of the item, avoiding purchase of new tags in the future. To increase the likelihood that migration and future operability will be maintained, the tags should not be locked, thus remaining 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. For more information, see Section 2.4.
- It is possible for newer RFID systems to recognize or be made to recognize multiple tag data formats. It is not necessary for libraries to convert 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.

4.2 Compatibility

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. 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—this compatibility does not guarantee interoperability. The air interface is the communication protocol between the tag and readers. 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 an important requirement. For libraries desiring migration to a standardized system, the issues are more complex.

Libraries with previously installed RFID systems need to address three issues of their system with their suppliers and vendors:

- Issue 1: Whether the RFID tags and readers are compliant with the ISO 18000-3, Mode 1 standard and can comply with Parts 1 and 2 of ISO 28560 as recommended in this document.
- Issue 2: Whether the various software systems can interpret and use the new standard data model.

- Issue 3: Whether the tag data format is partially or completely locked; if locked, the tag may not be reprogrammable to conform to the standard.

Some of the RFID tags in use in libraries today are compatible with ISO 28560 and 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 the library should understand for purposes of functionality.

First, it is not possible to upgrade a proprietary tag hardware design to an ISO 18000-3 Mode 1 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 or may not be possible to reprogram a proprietary RFID tag to comply with the standard. Depending on the vendor, it may be possible to reprogram a proprietary tag to store bits like the new standard tag. The capability of different systems to deal with this situation will vary, 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. Depending on the level of functionality desired, libraries can have a mix of compliant and non-compliant tags. A library with an existing collection tagged with proprietary tags could decide to switch to standardized tags and formats for their future acquisitions, and, if desired, migrate others only when items circulate. Over time, the collection would become predominantly and perhaps completely standards compliant. A library RFID vendor should be able to provide systems that would read multiple types of RFID tags and formats in the same library, thus supporting this approach.

4.3 Role of RFID Vendor

The library should expect that its vendor(s) 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 existing 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 upgraded software will support the new way that data will be stored on tags to conform to a standard, but 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 Role of Integrated Library System Vendor

As the industry adopts the new standards, the library who is ready to migrate, either wholly or over time, will also need to coordinate and discuss changes to tag programming with their ILS vendor and other RFID solutions vendors to ensure that the data necessary for use with the new model is available to each of the applications involved in the initial programming of tags and the circulation and processing of items. This may involve changes to the communication protocols used by these systems, such as NCIP and SIP2, to ensure the availability of relevant data and the accurate mapping of fields. Ideally changes to these protocols to fully support the new RFID standards will be built into future revisions of those standards, but interim localized tweaks by ILS and RFID vendors may be needed until that happens.

4.5 Suggested Migration Process

4.5.1 Migration Considerations

The need to migrate and the scope and speed of migration will depend on a number of factors, including ratio of new items to established items and the amount of conformity with the current system. A step-by-step migration path to a fully standard system can be developed with the assistance of your library

vendor. Many vendors already have some experience in this area, and can make some recommendations for a smooth transition process.

During the transition, most libraries will experience a period during which the collections contain both legacy RFID tags and new tags that reflect the new standards. They will thus be running with “mixed” tag environments.

There are several processes that can be used for migration. If existing tags can be reprogrammed, most library tag migrations will involve both “on the fly” (see 4.5.2) and “systematic” (see 4.5.3) changes in varying proportions.

In both the on-the-fly and systematic scenarios, 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, the RFID vendor, and the ILS vendor to ensure that the method of migration planned will be supported by the available upgrades. For instance, in the on-the-fly example discussed below, 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.

4.5.2 On-the-fly Migration

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 to the item, such as during a circulation operation.

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. Libraries should recognize, though, that automatic data migration is not magic. If the source data on the tag lacks data elements that are desired on the tag after the migration is complete, then the system performing the migration must be able to access the missing information from another system—or manual intervention may be necessary.

For the least impact on perceived system performance, it is worth considering reprogramming tags during check-in operations, when the patron is less impacted by the additional time considerations involved with adding this process. 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 sorting 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. Additionally, the sorting system can separate out any items that do not successfully reprogram and require staff intervention. You may need to schedule more time and staff to perform or monitor those check-in functions during the migration period.

The on-the-fly process will catch items that are most in circulation without having to place holds on popular items to change the tag programming. It will not catch all items and it may take a long time to reprogram less popular items, if this is your only approach to migration. 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 some time period following the start of the migration.

4.5.3 Systematic Migration

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.

In this scenario, library staff could: 1) 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, or 2) systematically remove groups of items from shelves to reprogram them at a desktop station, or 3) place holds on popular items to reprogram them as they were trapped. 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. A mixed approach of the three methods would likely speed the migration, especially since some materials circulate less frequently.

It is probably that a systematic migration would require more labor to implement than the on-the-fly method, yet it is quite likely that it would take less calendar time. It is recommended that a combination of both approaches be used to expedite the process. 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 transaction to help the borrowing institution.

4.6 Questions for RFID Vendors

Libraries considering purchase of an RFID system in the near future should be asking their vendors to explain their compliance with standards and, lacking that compliance, their planned migration path. They should also be able to tell how the configuration of their equipment will allow forward compatibility with this Recommended Practice. 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.

It is strongly recommended that US libraries only implement systems that are compliant with the ISO 28560-1 and ISO 28560-2 standards.

When purchasing, positive answers are needed to these questions:

1. Are the tags and readers compliant with ISO/IEC 18000-3 Mode 1?
2. If tags are purchased from other manufacturers, can the buyer 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?
3. Can new hardware, such as gates or self check-out stations, work with existing tags and existing hardware?
4. 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.

Section 5: The Book Supply Chain: The Value of Standardization

5.1 Introduction

In an increasing number of libraries, RFID tags are applied to facilitate the cycle of library operations, including the receipt, shelving, check-out, check-in, sorting and intra-system routing, re-shelving, inventory, and given goals for interoperability—potentially, interlibrary loans.

Libraries increasingly rely on distributors to ship material (books, CDs, and DVDs) fully processed and ready for the shelf, making it now possible for fully processed RFID items to reach patrons as quickly as possible. The processing includes the application of all types of labels (barcode, spine label, ownership label, etc.) and can include record uploads to a library's ILS (Integrated Library System) as well as the application of RFID tags and encoding to individual library specifications. Encoding may include the barcode number and other data as specified on the tag in lieu of encoding at the library. But lack of standardization has led to libraries adopting different and often proprietary RFID solution providers. In the absence of a predominant industry standard, distributors and jobbers have had to initiate different procedures for different customers, requiring the purchase, storage, and maintenance of different conversion stations, maintenance of multiple software licenses, and stocking of different tags, which makes it difficult for distributors to cost effectively apply and encode RFID for their customers.

5.2 Distributors and RFID Tag Applications

Costs to libraries may be limited if a standard tag and encoding methodology is embraced and adopted. In the absence of a standard in the past, costs for accommodating the varied equipment and data encoding for different libraries limited the cost-effective pricing of distributor tagging and encoding.

Issues include:

- Costs associated with the conversion stations – The distributors must purchase a conversion station for each vendor and costs will ultimately be borne by libraries requesting this pre-processing service.
- Valuable space required by conversion stations in the warehouse
- Equipment management issues – The distributor must manage the tags and conversion stations for each RFID solution provider.

One improving trend is that most RFID solution providers have standardized on the same ISO/IEC 18000-3 Mode 1 standard tag. But the distributor is still required to manage conversion stations for each vendor.

Standardization of the data model should 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 and data model issue has remained.

Figure 1 illustrates how the use of a standardized data model simplifies the programming process. Standardization will enable the Distributor to easily program the RFID chips independently of the RFID solution provider.

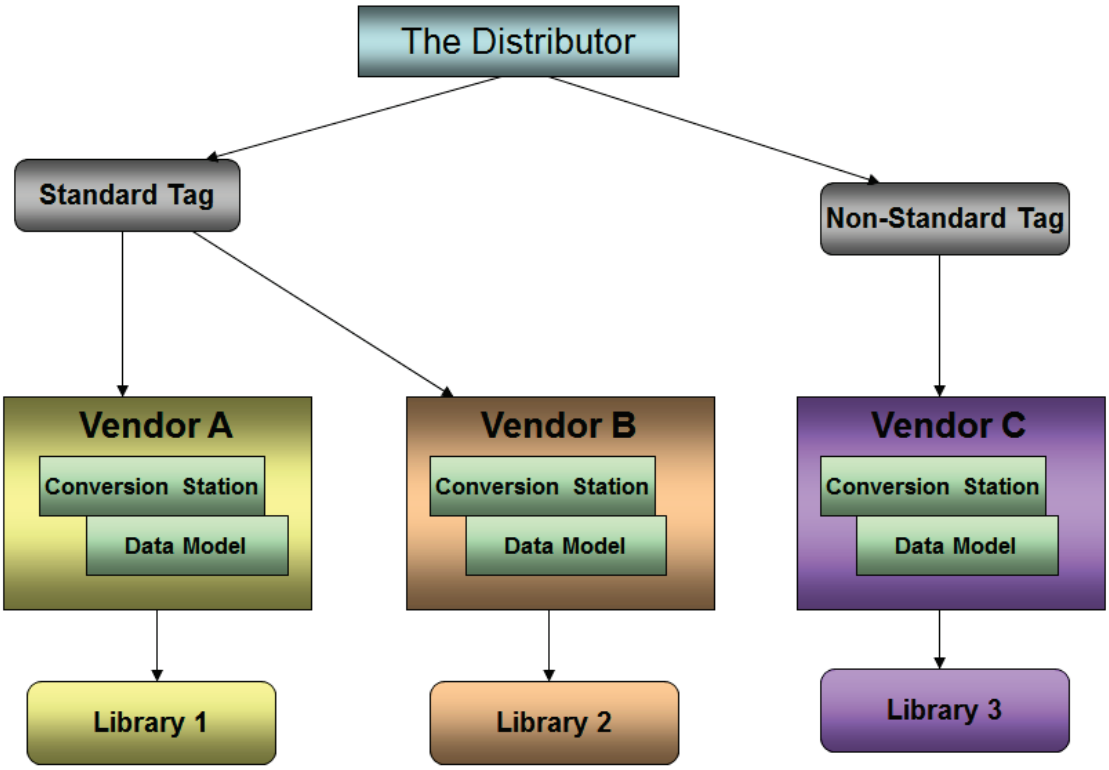

Figure 1: Distributor Applied RFID Tags

Figure 2 illustrates the issues facing distributors today. Until widespread adoption of the ISO 25860-2 standard by the industry, the distributor will, in many cases, be required to have a conversion station for each RFID solution provider vendor. Any mismanagement of the equipment can result in Vendor A's RFID tag being applied and programmed to books for a library needing Vendor B's tag. The error is only identified when the books are shipped to the library and the RFID tags cannot be read by the library's software. There is considerable urgency on the part of the wholesalers for this to change.

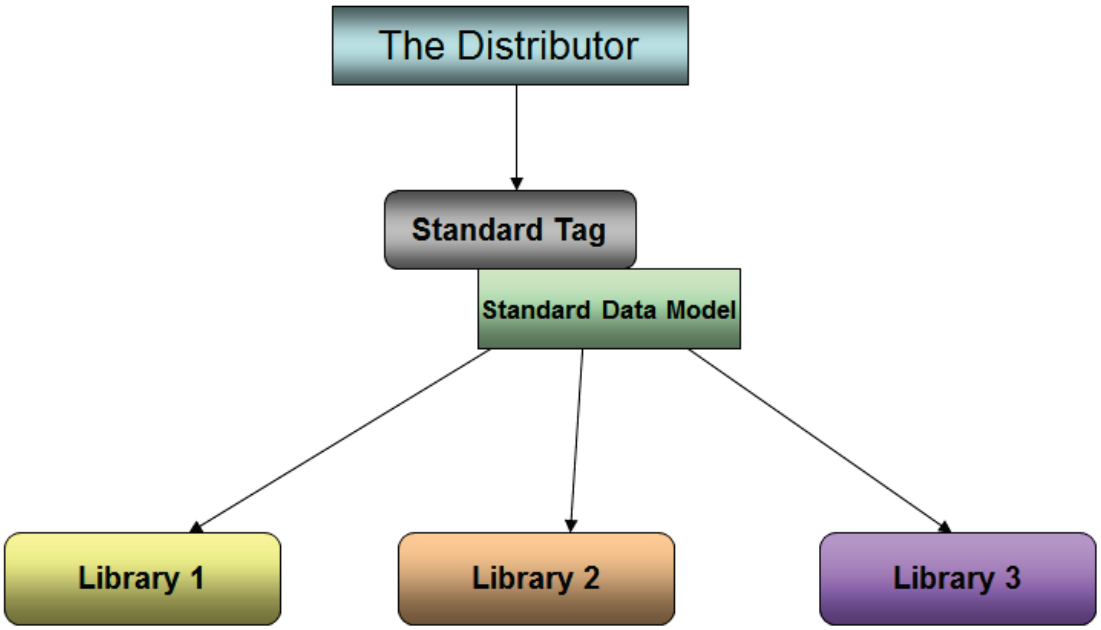

Figure 2: Standardized Data Model

The needs of the distributor in this discussion are very straightforward. Standardization of tags and data mapping will enable distributors to supply libraries with programmed tags at a more cost effective price. Without adoption of the ISO 28560 standard, distributors will have to maintain an inventory of equipment for each RFID solution provider. The cost of maintaining this equipment and labor to attach and program the tags specific to each vendor will be passed to the libraries. However, tags and data mapping that are standards compliant for interoperability will open up the possibility that distributors can use the same hardware and software for tags regardless of the RFID solution provider.

The problems faced by distributors are diminished as more RFID solution providers adopt standards, allowing the distributor to utilize a standard tag and programming scenarios on higher percentages of processed materials. The use of standards reduces the cost of providing RFID application services to libraries thus reducing the price to the libraries.

In summary, until a standard data model is adopted and an interoperable RFID market emerges, it will remain difficult for distributors to cost effectively satisfy the demand for applying and programming RFID tags for libraries.

The end goals of standardization include:

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

Section 6: Privacy

6.1 Privacy Issues

Library services in the United States are fundamentally characterized by an uncompromising institutional commitment to safeguard individual library patron privacy. Libraries stridently protect materials in their collections from censorship by individuals, groups, and representatives of municipalities and government—subject only to state, federal, and library policy conditions. In turn, library patrons rely on institutional adherence to principles that ensure their privacy is protected when reading materials in the library, using computers connected to the Internet, and, most relevant to RFID, when borrowing circulating materials.

The automated library circulation systems that replaced written tracking of patron checked-out materials were the first major computer programs developed to enable libraries to keep up with rapidly growing library circulation. These legacy systems began to be widely adopted in libraries during the 1980s. In time, progressive development of automated applications extended to additional library procedures including acquisitions, serials, patron requests, interlibrary loan, and other functions as the legacy systems evolved to today's Integrated Library System (ILS). With the increasing strides in automating repetitive and routine clerical activities in libraries, however, the requirement to protect the privacy of library patron transactions from review by anyone other than authorized library personnel has remained a fundamental design criterion. Deployment of RFID requires the same vigilance to ensure patron privacy is protected.

In spite of the fact that RFID has shown great promise in further streamlining the circulation and handling of library materials during times of increasing library use and declining library funding, it is not surprising that RFID has been subject to close scrutiny and concern about how this technology can be deployed without undermining a library patron's privacy. RFID's potential for shifting the check-out and check-in of materials to patrons, rather than staff, and automating the sorting of returned library materials in libraries with multiple branches and large collections touch on patron privacy when a patron is linked by an RFID system with the circulation of an item.

The library community's response to the continuing viability of increasing use of RFID in libraries ultimately resulted in activities within the affected professional associations and groups aligned with the broader library industry. 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, distributors, distributors, and technology vendors.

6.2 ALA Resolution on RFID Technology and Privacy

Completed in late 2004, and subsequently adopted by BISG and ALA, the *ALA Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles* has five main tenets. It states:

> 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.

The policy also resolved that the ALA develop implementation guidelines for the use of RFID technologies in libraries.

Following the resolution, ALA's Intellectual Freedom Committee was asked to examine the technology on a more detailed level with the intention of adopting a new set of "Confidentiality Guidelines." It was envisioned that the new guidelines could be used by libraries to guide their adoption of RFID technology in a manner that ensured that relevant privacy issues the Committee felt appropriate would be addressed. The committee conducted meetings and considered comments from association members and others.

6.3 ALA Guidelines on Privacy and Confidentiality in RFID

RFID in Libraries: Privacy and Confidentiality Guidelines, adopted by the ALA Intellectual Freedom Committee on June 27, 2006, responded in part to concerns that because "RFID tags may be read by unauthorized individuals using tag readers, there are concerns that the improper implementation of RFID technology will compromise users' privacy in the library" and that researchers "have identified serious general concerns about the privacy implications of RFID use, and particular privacy concerns about RFID use in libraries." The most relevant sections in the *Guidelines* for this discussion are the "Policy Guidelines" and "Best Practices" sections.

The "Policy Guidelines" section emphasizes a library's obligation to inform and educate library staff and members of its community about all aspects of the intended deployment of RFID. A library is encouraged to have a "transparent (RFID) selection process" and to "publicize its reasons for its planned implementation while considering comments from the library's users to broaden the public debate," if any, over the proposed implementation. Libraries are charged to "review and update appropriate privacy policies and practices addressing notice, access, use, disclosure, retention, enforcement, security, and disposal of records" that are reflected in the configuration of the RFID system. In summary, the library should engage in thorough public and staff education, including review and discussion of all aspects of a planned implementation.

This section also encourages libraries to consider procuring systems that would allow library patrons to choose whether to use RFID technology or "opt out," and use another system for circulation. This choice would require a library to operate two parallel systems for circulation, however. Libraries are also encouraged to "delete personally identifiable information collected by RFID systems, just as libraries take reasonable steps to remove personal information from aggregated, summary data."

The "Best Practices" section of the *Guidelines* reinforces the privacy tenets of the ALA Council policy and provides increased technical specificity. Libraries are encouraged to extend the same commitment and practices affecting security of bibliographic and patron databases used in an ILS to a planned RFID deployment, and to "use the most secure connection possible for all communications with the ILS to prevent unauthorized monitoring and access to personally identifiable information." Any data stored on an RFID tag should be "protected by the most secure means available, including encryption."

Further, libraries should "block the public from searching the catalog by whatever unique identifier is used on RFID tags to avoid linking a specific item to information about its content," and staff should be trained "not to release information about an item's unique identifier in response to blind or casual inquiries." Consistent with the ALA Council's *Technology Principles,* libraries are advised not to store any personally identifiable information on any RFID tag. The only area of disagreement with this document's proposed practices pertains to the determination by the Intellectual Freedom Committee that libraries should "limit the bibliographic information stored on a tag to a unique identifier for the item (e.g., barcode number, record number, etc.)." A method for storing limited bibliographic information on an RFID tag is suggested as an optional use in this document.

6.4 Implementing the NISO RFID Recommendations and ALA RFID Policy

The most critical aspect of both the ALA Council's *RFID Technology Principles* and the Intellectual Freedom Committee's *Privacy and Confidentiality Guidelines* is that a library should engage in a thoroughly open and transparent examination of all aspects of how RFID may be deployed so that patrons and staff can examine all aspects of the proposed deployment, with an emphasis on understanding how the technology ensures patron privacy. Such an examination should provide the best forum for examining all areas where trade-offs between a decision to utilize RFID tag fields to store bibliographic or other data, provided as an optional use as outlined in this document, is weighed against only storing a unique item identification number as suggested in the Intellectual Freedom Committee's *Privacy and Confidentiality Guidelines.*

It is important to note that this Recommended Practice document (*RFID in U.S. Libraries*) concurs that no patron information should be stored on an RFID tag and that no transactional data regarding patron use be stored in any case. Individual libraries are in the best position to determine what is best for their patrons and communities. *RFID in U.S. Libraries* does provide recommendations to enable this technology to be used efficiently and effectively without compromising library privacy and confidentiality.

Section 7: Vandalism

7.1 Introduction

As with any library materials or equipment, RFID systems have some vulnerability to the few individuals in society intent on vandalizing public property. 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 of 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 protective qualities of 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 from the exposure they encounter just by maintaining their collections with open doors and their catalogs accessible online.

Note that 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 an RFID reader. An individual with malicious intent could also 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. More and more commonly, hand held devices like PDAs and smartphones can interact directly with RFID tags. With the proliferation of these handheld devices, the opportunity for mischief increases. As a result, the risk of this type of vandalism occurring also increases. Libraries are advised to consider these risks and develop a position most suitable for their environment.

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, i.e., exchanging item numbers, for the purposes of theft. Any of these situations causes difficulty to the library. Programming and locking the primary item identifier (see Section 2.5.2) will enable the library to protect against modification of tag contents. Data objects that have been altered by a vandal may be reconstructed, as long as the primary identifier is still intact.

7.4 RFID Viruses

There have been some discussions 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.[3] 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, the Working Group is unaware of any such attacks against existing library RFID systems. Furthermore, some time has passed since the emergence of these theoretical threats, and the Working Group is also not aware of any practically successful attacks made on 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, it is expected that systems will continue to be hardened against such attacks.

7.5 Intentional Detuning of the Tag

The low-tech method of defeating the security functionality of an RFID tag 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.

7.6 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 without obviously damaging the item. Short of changes such as this, the tags remain visible and accessible to the vandal. Some libraries have found their tags vulnerable to the fingers of small children who like stickers.

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. 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.

[3] 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.

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 have improved 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.

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. 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. Particular care should 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 bookshelves.

Placement of currently deployed high frequency (HF) tags is a critical factor affecting system performance (see Figure 3 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 tag's resonant 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 3: 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, 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, unless AFI is locked	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, unless AFI is locked	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, unless AFI is locked	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 and on which the AFI code is not locked 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 and on which the AFI code is not locked 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: UHF RFID in Libraries

C.1 Introduction

In the past there have been concerns about UHF RFID for item level identification in libraries. The 2007 edition of *RFID in U.S. Libraries* by this NISO working group included this prediction:

> Most of the above limitations on the 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.[1]

As of the publication of this new edition of the NISO data model for U.S. libraries, there is no standard for RFID in libraries at UHF frequencies. All existing UHF implementations, like most HF library ones, are proprietary implementations. This appendix is intended to document current activities in other parts of the world and examine what is happening with UHF implementations in the book and library industries.

Alan Butters, principal consultant with Sybis, published a thoughtful report in 2008 examining the issues of UHF technology for libraries.[2] In this report he considers estimated cost savings through increased production volume of UHF tags. He also addresses performance advantages of UHF for significantly greater read range and immunity against tag masking (close proximity of tags). Butters also mentions the possible advantages for libraries if there is further UHF deployment in the publishing supply chain (see more in the following).

C.2 Book Retail and Publishing UHF RFID – Implications for Libraries

In 2006, with the release of a new EPC Gen2 standard that revived the possibility of item-level tagging with UHF RFID, the publishing industry started to experiment with the technology. Boekhandels Groep Nederland (BGN) the largest book retailer in The Netherlands, opened the world's first fully-automated item-level UHF RFID tagged store at Almere in April 2006 and the second one at Maastricht in October of the same year. These Selexyz-branded smartstores were reporting accuracy approaching 100% and the sale volumes increased by 50%.[3] These installations have rewarded the bookseller with the RFID Visionary Award for 2006 at the RFID Breakthrough Awards in London. BGN won the Torex Retail ICT Award and was recognized by *InfoWorld Magazine* as one of the 100 most significant IT projects of 2006.[4] In April 2007, BGN expanded its RFID project by installing RFID antennas on the shelves for the special-order books in its two RFID-enabled stores, thus making item-level tracking enabled.[4] In December 2008, it was reported in the press release of BGN's RFID solution provider that BGN has increased inventory visibility across its chain from 65% to 97.5% with an accuracy of 100%.[5]

In further supply chain efforts, the Japanese publisher Shogakukan reported using UPM Raflatac UHF EPC Gen2 Crab inlays to help them improve tracking the high rate of book returns (47%) in Japan in 2009.[6 and 7]

C.3 UHF RFID in Libraries

As of the time of writing this report, only two U.S. libraries were identified as considering UHF RFID. The Carver County Library in Waconia MN has been conducting some tests with 3M, but do not have current plans for implementation. However, the Grand Rapids Public Library with Calvin College and Bibliomation are actively pursuing development of an open-source UHF RFID solution planned for 2012-13.[8]

In just three years since the NISO Report, UHF RFID implementations have emerged in Australia, Singapore, and Hong Kong and trial projects in China. Civica and Adilam Technologies reported in October 2006 on their implementations in five libraries in Singapore and Australia utilizing their Spydus

software system with RFID supplied by Alien Technology Corporation.[9] These installations are EPC Global Gen2 standard tags that read across the 860-960MHz UHF spectrum at top speeds of 1000 tags per second.

Also in 2006, the City University of Hong Kong implemented two parallel library pilots to test both HF and UHF RFID.[10] Their findings indicated their success with UHF RFID and future selection. The library research team was able to control the read range and orientation of RCW's UHF RFID readers and antennas through design of a proprietary read-range controlling device (patents pending in Hong Kong, China, and Taiwan).

In August 2010, the City University of Hong Kong Library has been recognized as a founding leader in a cross-border collaboration between China and Hong Kong libraries to establish the UHF RFID Application Working Group for a UHF data model for libraries and explore interoperability standards.[11] Other founding members include Tsinghua University and Shanghai Jiao Tong University libraries. This group has been joined by libraries from Shantou University, the National Library of China, Chinese University of Hong Kong, Baptist University of Hong Kong, and the GS1 Hong Kong.

Appendix D: Encoding Data on the RFID Tag

D.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 formal 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.

Guidelines have been developed to assist those involved in implementing ISO 28560-compliant encoding systems. These guidelines are available on-line at the following address: http://biblstandard.dk/rfid/docs/conformance_28560-2.pdf. Helpful examples are included to illustrate technical concepts like proper byte order and the correct structure of a data element.

D.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. According to ISO 28560-2, 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 of 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.

D.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	U.S. 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 4. 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 D.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.

D.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	Variable
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	Variable
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.

D.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 encoding of the Owner Library/Institution data element is specified by special rules defined in ISO 28560-2. These rules are used to obtain a very efficient encoding of the ISIL, and are dependent upon the specifics of the data element definition as described in the ISO 15511 specification. The rules are described in detail in that document, in Appendix C, and not reproduced here.

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

Table 6: Compacting an ISIL Code, example 1

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	000 Application defined

Data Object	Owner Library/Institution
Encoded Bytes	ACC09EBAA06F6B Length: 7 bytes

An additional example of an ISIL code in Table 7 is based upon the OCLC code for the Library of Congress.

Table 7: Compacting an ISIL Code, example 2

Data Object	Owner Library/Institution
Relative OID	3
Data Format	Alphanumeric Per ISO 15511
Specified Length	Max 16 characters
Example of User Data	OCLC-DLC Length: 8 characters
Compaction Scheme	000 Application defined
Encoded Bytes	78D8301183 Length: 5 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.

D.3.3 Set Information

The set information is presented in two components: The number of parts followed by the ordinal part number. 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 8. If the total number of parts is between 100 and 255, then the user data is presented as a 6-digit code.

Table 8: Compacting the Set Information

Data Object	Set Information (ordinal part number; number of parts)
Relative OID	4
Data Format	Numeric
Specified Length	2, 4, or 6 digits
Example of User Data	1204 Length: 4 digits
Compaction Scheme	001 integer
Encoded Bytes	04B4 Length: 2 bytes

D.3.4 Shelf Location

The first example (Table 9) uses a Library of Congress Catalog classification.

Table 9: Compacting the Shelf Location Based on the Library of Congress Catalog Classification

Data Object	Shelf Location
Relative OID	6
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 10).

Table 10: Compacting the Shelf Location Based on a Local Scheme

Data Object	Shelf Location
Relative OID	6
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.

D.3.5 GS1 Identifier

The GS1 Identifier 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, 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 11 is of a 13-digit ISBN.

Table 11: Compacting the GS1 Identifier

Data Object	GS1 Identifier
Relative OID	13
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.

D.3.6 Title

The example in Table 12 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 12: Compacting the Title

Data Object	Title
Relative OID	17
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.

D.3.7 Order Number

An example of the compaction of an order number is shown in Table 13. 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 13: Compacting the Order Number

Data Object	Order Number
Relative OID	10
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

D.3.8 Supplier Identifier

The example in the Table 14 shows the compaction of a supplier identifier—in this case, the name of the supplier's business.

Table 14: Compaction of the Supplier Identifier

Data Object	Supplier Identifier
Relative OID	9
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 when the item is first registered in the library loan system.

D.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/IEC15961 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 15, the following three data elements are encoded on the RFID tag:

- Relative-OID 3 ISIL
- Relative-OID 6 Shelf location
- Relative-OID 15 Local Data – A

These three Relative-OIDs {3, 6, 15} require the OID index to have the following bits set to equal 1 {1st, 4th, 13th}. 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 15: 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	Variable length
Example of User Data	1001000000001000 Length: 2 bytes
Compaction Scheme	000 User-Defined
Encoded Bytes	9004 Length: 2 bytes

D.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.

D.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 4. The relative OID values 1 to 14 are directly encoded in the Precursor, and this reduces the amount of memory required for the encoding.

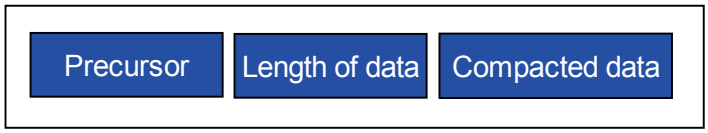

Figure 4: Data Set Structure for Relative-OID Values 1 to 14

D.4.2 The Precursor

For the library applications, the Precursor is a single byte with the bit structure as defined in Figure 5.

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

Figure 5: Bit Position of Precursor Components

- The **Offset** is associated with the need to align blocks when a data set has to be locked (see this Appendix Section D.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.

D.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.

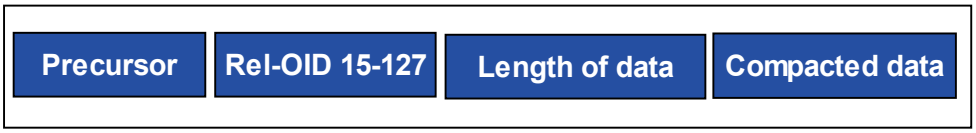

Figure 6: Data Set with Relative OID 15 to 127

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}".

D.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 from the encoding rules of ISO/IEC15962, but these are associated with different object identifier structures, or can apply when data is locked.				

Taking the worked examples in Sections D.3.1 to D.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	03	07	ACC09EBAA06F6B
ISIL Code	Table 7	03	05	78D8301183
Set Information	Table 8	24	02	04B4
Shelf Location	Table 9	46	07	441CB6E2E335D6
Shelf Location	Table 10	36	07	324747B1692B80
GS1 Identifier	Table 11	1D	06	08E77163DE4D
Order No	Table 13	4A	07	042C72CF4D6D62
Supplier Identifier	Table 14	59	0E	85BF7EB412B7E2C59792093BB1FF
OID Index	Table 15	02	02	9004

*

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

Data Element	Example from:	Precursor	Relative OID	Length of Compacted Data	Compacted Data
Title	Table 12	5F	02	18	872A5D64127766DFCB6E1 E9A77EE414396FC7979F3 D3BB3F

D.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 in Figure 7 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 (See example in D.6.3).

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. This is illustrated in the following examples.

The difficulty involved in editing data elements residing in tag memory is readily apparent to a system designer. These difficulties are exacerbated when the tag memory becomes fragmented by locked data elements, particularly when there are multiple noncontiguous blocks in tag memory which are locked. Because of these complications, it is our recommendation that any locked data elements with OID greater than 2 be physically located immediately after the OID Index data element. This practice will result in a contiguous locked section containing one or more data elements, and data elements which will remain unlocked can be placed beyond that section in physical tag memory, easing the burden on a system which attempts to edit these elements.

D.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 Title 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	Relative OID	Length of Compacted Data	Compacted Data
Primary Item ID	Yes	11		06	0B3A73CE2FF2
OID Index	No	02		02	9002
Shelf Location	No	46		07	441CB6E2E335D6
ISIL Code	Yes	03		07	ACC09EBAA06F6B
Title	No	5F	02	18	872A5D64127766DFCB6E 1E9A77EE414396FC7979 F3D3BB3F

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.

D.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.

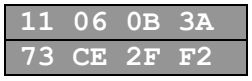

Figure 8: Encoding the Primary Item Identifier

D.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.

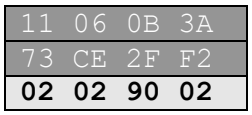

Figure 9: Encoding the OID Index

D.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

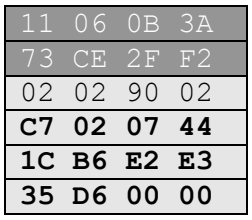

Figure 10: Encoding the Block-aligned Shelf Location

D.6.4 Encoding the ISIL Code

The data set for the ISIL code is 9 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 02_{HEX} and encoding two null bytes—value 00_{HEX}—following the data. The resultant encoding is shown in Figure 11.

11 06 0B 3A
73 CE 2F F2
02 02 90 02
C7 02 07 44
1C B6 E2 E3
35 D6 00 00
83 02 07 AC
C0 9E BA A0
6F 6B 00 00

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

D.6.5 Encoding the Title

Note that this example is included because it represents encoding a data set with an OID between 15 and 127. This Best Practice, by demonstrating how to encode the title, is not making a recommendation to encode that data element. The data set containing the Title 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 90 02
C7 02 07 44
1C B6 E2 E3
35 D6 00 00
83 02 07 AC
C0 9E BA A0
6F 6B 00 00
5F 02 18 87
2A 5D 64 12
77 66 DF CB
6E 1E 9A 77
EE 41 43 96
FC 79 79 F3
D3 BB 3F 00

Figure 12: Encoding the Title

D.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 decoding 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 of Acronyms

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 Z39.83-2008. 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 and revised in 2008. 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

3M Standard Interchange Protocol, version 2.0 [SIP2]. 3M Library Systems, updated April 11, 2006. Available at: http://multimedia.3m.com/mws/mediawebserver?mwsId=SSSSSu7zK1fslxtUm8_9m82Uev7qe17zHvTSevTSeSSSSSS--&fn=SIP2%20Protocol%20Definition.pdf

American Library Association. *RFID in Libraries: Privacy and Confidentiality Guidelines*. Adopted by the Intellectual Freedom Committee, June 27, 2006. Available at: http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=130851

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

ANSI/NISO Z39.43-1993 (R2011), Standard Address Number (SAN) for the Publishing Industry. Baltimore, MD: National Information Standards Organization, 1993. Available at: http://www.niso.org/standards/z39-43-1993r2006/

ANSI/NISO Z39.83-1-2008, *(NISO) Circulation Interchange, Part 1: Protocol (NCIP)*. Baltimore, MD: National Information Standards Organization, 2008. Available at: http://www.niso.org/standards/z39-83-1-2008/

ANSI/NISO Z39.83-2-2008, *Circulation Interchange, Part 2: Protocol Implementation Profile 1*. Baltimore, MD: National Information Standards Organization, 2008. Available at: http://www.niso.org/standards/z39-83-2-2008/

Butters, Alan. *New RFID Technologies & Standards – What Does It All Mean for Your Library?* Presented at: VALA 2008 14th Biennial Conference and Exhibition: Libraries / changing spaces, virtual places, Melbourne, Australia, February 5-7, 2008. Available at: http://www.valaconf.org.au/vala2008/papers2008/66_Butters_Final.pdf

Ching, Steve H., and Alice Tai. *HF RFID versus UHF RFID-Technology for Library Service Transformation at the City University of Hong Kong*. The Journal of Academic Librarianship, 35(4), July 2009, pp. 347-359. [It is also notable that the Library was awarded the *Certificate of Merit* for the 2008 RFID Awards from GS1 Hong Kong.] Available at: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6W50-4WJ2CGV-1&_user=10&_coverDate=07%2F31%2F2009&_rdoc=1&_fmt=high&_orig=gateway&_origin=gateway&_sort=d&_docanchor=&view=c&_searchStrId=1745871250&_rerunOrigin=google&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=8ca8d1a28778ec721ca37848faaefa23&searchtype=a

CityU and mainland university libraries explore UHF RFID data model standardisation. City University of Hong Kong press release, August 20, 2010. Available at: http://wikisites.cityu.edu.hk/sites/newscentre/en/Pages/201008201721.aspx

DS/INF 163-1:2005, *RFID Data Model for Libraries*. Charlottenlund, Denmark: Dansk Standards, 2005. Available at: http://webshop.ds.dk/product/M206308/standard.aspx

Dutch bookstore chain builds world's first fully automated item-level RFID tagged store, with Progress Software technology. Supply Chain Management, May 5, 2006. Available at: http://www.logisticsit.com/absolutenm/templates/article-supplychain.aspx?articleid=2079&zoneid=5

Ehlers, Marla (Grand Rapids Public. Library, Grand Rapids, MI). *In October 2006,Civica and Adilam Technologies, two software and RFID players in Australia, jointly announced that their UHF RFID library applications have been installed in five different libraries in Australia and Singapore.* E-mail message thread with Corrie Marsh (The University of Texas – Pan American), July 19-20, 2010. Note: These five libraries were: Blacktown City Council Library, NSW, Australia; Victor Harbor Public Library, SA, Australia;

Loreto Mandeville Hall, VIC, Australia; Nanyang Girls' High School, Singapore; and Camden Council Library Service, NSW, Australia.

EPC™ Radio-Frequency Identity Protocols: Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz, version 1.2.0. EPCglobal Inc., October 23, 2008. Available at: http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf

IETF RFC 3629 UTF-8, *A Transformation Format of ISO 10646*. Internet Engineering Task Force, November 2003. Available at: http://tools.ietf.org/html/rfc3629

ISO 15511: 2009, *Information and documentation – International Standard Identifier for Libraries and Related Organizations (ISIL)*. Geneva: International Organization for Standardization, 2009. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=52666

ISO 28560-1:2011, *Information and documentation – RFID in libraries – Part 1: Data elements and general guidelines for implementation.* Geneva: International Organization for Standardization, 2011. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50996

ISO 28560-2:2011, *Information and documentation – RFID in libraries – Part 2: Encoding of RFID data elements based on rules from ISO/IEC 15962*. Geneva: International Organization for Standardization, 2011. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50997

ISO 28560-3:2011, *Information and documentation – RFID in libraries – Part 3: Fixed length encoding*. Geneva: International Organization for Standardization, 2011. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50998

ISO/IEC 646:1991, *Information technology – ISO 7-bit coded character set for information interchange*. Geneva: International Organization for Standardization, 1991. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4777

ISO/IEC 10646: 2011, *Information technology – Universal Coded Character Set (UCS)*. Geneva: International Organization for Standardization, 2011. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51273

ISO/IEC 15961:2004, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface.* Geneva: International Organization for Standardization, 2004. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30528

ISO/IEC 15962:204, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions.* Geneva: International Organization for Standardization, 2004. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30529

ISO/IEC 15693-1:2010, *Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 1: Physical characteristics*. Geneva: International Organization for Standardization, 2010. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39694

ISO/IEC 15693-2:2006, *Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 2: Air interface and initialization*. Geneva: International Organization for Standardization, 2006. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39695

ISO/IEC 15693-3:2009, *Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 3: Anticollision and transmission protocol*. Geneva: International Organization for Standardization, 2009. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43467

ISO/IEC 18000-3:2010, *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, 2010. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=53424

Japanese Publisher Shogakukan Implements RFID Solution Using UPM Raflatac Tags to Reduce Return Ratios and Waste. MoreRFID, December 10, 2008. Available at: http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=5270&display=RFID

Molnar, David, and David Wagner. *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. Available at: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.71.6371

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

ONIX for Books Codelists, Issue 16 for Release 2.1 and 3.0. EDItEUR, January 27, 2012. Available at: http://www.editeur.org/14/Code-Lists/

Progress Software Customer BGN Wins Prestigious RFID Visionary Award at 2006 RFID Breakthrough Awards. MoreRFID, November 20, 2006. Available at: http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=2355&display=RFID

RFID enables book distribution system. RFIDNews, December 4, 2008. Available at: http://www.rfidnews.org/2008/12/04/rfid-enables-book-distribution-system

Rieback, M. R., B. Crispo, and A. S. Tanenbaum. *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. Available at: http://doi.ieeecomputersociety.org/10.1109/PERCOM.2006.32

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

Sensormatic® Item-Level Intelligence Solutions from ADT® Boost Sales at the Netherlands' Largest Bookseller. Boca Raton: Sensormatic Press Release, December 8, 2008. Available at: http://www.sensormatic.com/whoweare/prDetailprint.aspx?id=234

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

UHF RFID – Libraries Taking the Next Step into the Future. Civica and Adilam Technologies joint press release, October 2006. Available at: http://www.adilamtech.com.au/library/Why_UHF.pdf

UK Library Operations Profile for ISO 28560-2. Book Industry Communication, March 2010. Available at: http://www.bic.org.uk/e4librariesfiles/pdfs/111102%20UK%20Data%20Model%20for%20RFID%20in%20Libraries%20updated.pdf