A Progress Report on NISO’s work on

RFID Standards in Libraries

ALA Seattle, January 21, 2007

Vinod Chachra, PhD
Chairman, NISO Standards Committee on Library Applications of RFID
CEO, VTLS Inc.
NI SO RFID Standards Committee

Following types of organizations are participating in the working group:

1. RFID hardware manufacturers
2. RFID solution providers (software and integration)
3. RFID Library users
5. Other related organizations
Committee Members

Livia Bitner, Baker & Taylor
Vinod Chachra, VTLS – Committee Chairman
Brian Green, EDItEUR
Jim Litchenberg, BISG
Alastair McArthur, Tagsys
Allan McWilliams, Baltimore County Public Library
Louise Schaper, Fayetteville Public Library
Paul Sevcik, 3M
Paul Simon, Checkpoint
Rick Weingarten, ALA
Marty Withrow, OCLC
Scope of NISO RFID Standards

- RFID solutions run at several frequencies –
  - Low – from 125KHz to 134KHz
  - High – 13.56MHz
  - Ultra High – 860-960 MHz
  - Micro Wave – 2.45 GHz

- NISO’s work is limited to Tags used in libraries

Note: At present, these tags operate at 13.56 MHz, though this may change in the future.
Goals of NISO Standards Group

To **review** existing RFID standards… and promote its use where appropriate;

To examine and assess **privacy concerns**;

To investigate the way RFID is used in the United States and identify best practices in **standards development and implementation**;

To focus on security and **data models** for RFID tags, along with issues of **interoperability** and privacy;

To create a “**best practices**” document for libraries … and help safeguard library investments in RFID and minimize the cost of obsolescence.
Functions Examined

Supply Chain Tracking
  Item Level Tagging
  Carton Level Tagging
  Application of tags by book jobbers
  Application of tags by libraries

Self Checkout Stations

Book drops

Sortation systems

Inventory systems

Media tagging

ILL functions
Functions Examined

Supply Chain Tracking
  Item Level Tagging
  Carton Level Tagging
  Application of tags by book jobbers
  Application of tags by libraries
Self Checkout Stations
Book drops
Sortation systems
Inventory systems
Media tagging
ILL functions
Publisher uses carton level barcode and ASN transaction to provide shipment information to wholesaler.

Jobber uses carton level barcode and ASN transaction to receive books from the publishers. Provide ASN transactions to libraries.

With the use of an ILS developed module, the Library uses carton level barcode and ASN transaction to receive books from the wholesalers.

Library Applied RFID Tags
Library applies proprietary tag and programs RFID tag with proprietary conversion station for use in library applications.

Barcode contains with item identifier for use at different levels of supply change.

Barcode used to track books in warehouse.

Barcode used to track books in warehouse.
Jobber applied RFID Tags

The Jobber

Vendor A
RFID tag
Hardware
Software
Library uses RFID Vendor A

Vendor B
RFID tag
Hardware
Software
Library uses RFID Vendor B

Vendor C
RFID tag
Hardware
Software
Library uses RFID Vendor C

Jobber maintains conversion stations for each RFID vendor to program RFID tag.
Publisher uses carton level **RFID tag** and ASN transaction to provide shipment information to jobber.

Jobber uses carton level **RFID tag** and ASN transaction to receive books from the publishers. Provide ASN transactions to libraries.

The **Publisher** programs the embedded **RFID tag** with item identifier.

Uses the item identifier in the embedded **RFID tag** for tracking book in warehouse.

**Jobber Supplied RFID tags**

- Jobber programs RFID tags in a batch process and applies to each library’s books independent of Library’s RFID Vendor.

- Library uses RFID Vendor A
- Library uses RFID Vendor B
- Library uses RFID Vendor C
- Library uses RFID Vendor D

Embedded **RFID tag** enables use at different levels of the supply chain.
Functions Examined

Supply Chain Tracking
  Item Level Tagging
  Carton Level Tagging
  Application of tags by book jobbers
  Application of tags by libraries
Self Checkout Stations
Book drops
Sortation systems
Inventory systems
Media tagging
ILL functions
Privacy Concerns

Proper caution and concern raised by some privacy advocates … including EFF (Electronic Frontier Foundation)

Exaggerated concerns raised by others.

Issue is very sensitive for it can

- potentially cause privacy problems and/or
- possibly derail or slow down RFID implementations and/or
- add to the implementation costs

Organizations like BISG, EFF and American Library Association are providing leadership in this area.
Privacy Concerns

EFF (Electronic Frontier Foundation) says:

While RFIDs are a convenient way to track items, they are also a convenient way to do something far less benign: track people and their activities through their belongings. EFF is working to prevent the embrace of this technology from eroding privacy and freedom.

EFF also highlights reports of the ‘hackability’ of RFID chips which appears to have inspired their epithet: ‘privacy-leaking’. Among EFF’s priorities is to keep these ‘privacy-leaking’ chips out …
Privacy Concerns

Similar concerns were also reflected in a piece in Wired magazine (May 2006) entitled “The RFID Hacking Underground” which included a variety of comments and opinions.

David Molnar ... a computer science graduate student who studies commercial uses for RFIDs at UC Berkeley.... discovered he could destroy the data on the books' passive-emitting RFID tags by wandering the aisles with an off-the-shelf RFID reader-writer and his laptop.
Privacy Concerns

Center for Democracy and Technology (CDT Group). Among the recommendations –

• notify customers in all cases when RFID technology is being used;

• inform customers whether they can deactivate the tags, and

• build security into the technology as an essential design element.

Privacy - Technology Perspective

- RFID tags are powerless; without power they are inert and inactive
  
  When a tag reader comes close it charges the tag
  
  The tag then transmits the data to the reader

- RFID tags used in libraries have a short read range

  Range is 8 to 18 inches

  This small read range is important to the application as we do not wish to “influence” the tags on the book shelves while dealing with the tags on checkout or checkin stations
RFID Privacy Principles

(This is a direct quote from the BISG web site)

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:

1) 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.

2) Ensure that no personal information is recorded on RFID tags which, however, may contain a variety of transactional data.
3) Protect data by reasonable security safeguards against interpretation by any unauthorized third party.

4) Comply with relevant federal, state, and local laws as well as industry best practices and policies.

5) Ensure that the four principles outlined above must be verifiable by an independent audit.

This policy has been developed and released by the Book Industry Study Group in cooperation with the American Library Association, Office of Information Technology and the Office for Intellectual Freedom, as well as the National Information Standards Organization.
Vandalism

RFID Systems in libraries are vulnerable to electronic vandalism.

- Modification of security information to steal an item
- Permanent locking of security bits or AFIs
- Modification of tag contents as vandalism
- Modification of tag contents to steal an item
- Permanent locking of other fields after modification
- RFID Viruses
- Physical defacing or removal of the tag
Responses to Vandalism

There are several sources of potential help with the various attacks available to vandals.

- Criminal penalties against the perpetrators of vandalism, if they can be identified and prosecuted.
- Password protection schemes on data which must remain changeable during the life of the item
- Simple locking on static data
Perspective on Vandalism

Responses to vandalism are likely to hinder interoperability, and place the library only a few steps ahead of increasingly sophisticated vandals.

Libraries must ultimately choose whether the impediments presented to vandals outweigh the detrimental impacts of the protections.

Different libraries are likely to find the balance point in different positions on this issue, and there is really no right or wrong choice that every library will adopt.

For many libraries, the least expensive solution may be to accept the basic risks associated with RFID as an incremental difference over the exposure they encounter just by maintaining their collections with open doors.
Interoperability (from Whatis.com)

Interoperability (pronounced IHN-tuhr-AHP-uhr-uh-BIHL-ih-tee) is the ability of a system or a product to work with other systems or products without special effort on the part of the customer. Interoperability becomes a quality of increasing importance for information technology products as the concept that "The network is the computer" becomes a reality. For this reason, the term is widely used in product marketing descriptions.
Interoperability Level 1

Level 1: Within the Library

Tags: The fear that the tags purchased may not be useful or available in the future requiring expensive and time consuming retagging operations.

Suggested solutions

• Standardization of tags.
• Standardization of the data on the tag
• Tags purchased from other manufacturers should interoperate with the existing standardized tags
• Existing hardware and software be used with the new tags without any (or major) re-engineering?
Interoperability Level 1

Level 1: Within the Library

**Hardware interoperability:** If the library purchases additional hardware like new gates or new self check units from a manufacturer different from the original supplier, then can this new hardware interoperate with existing tags and existing hardware?

**Software interoperability:** Can the library swap out software with different or better functionality without changing the tags or hardware?

This level of interoperability will allow libraries to purchase the best systems to match their needs, choosing components from different suppliers when this makes the best sense.

Expanded options for replacement equipment will become available if compatibility with an existing installed base of tags can be accomplished through standardization.
Interoperability Level 2

Level 2: Within the community

It is very desirable that library tags do not set off alarms in book stores and grocery stores.

The reverse is true too. Librarians would not like grocery store items to set off alarms in the libraries.

Solution:

The AFI (Application Family Identifier -- discussed in the security section) is a perfect mechanism to control this aspect of operations.

The committee strongly recommends that only tags based on AFI technology be used in libraries.
Level 3: ILL purposes

A tag from library A should be able to service the circulation needs of library B.

Solution:

Use of standards based tags

Use of standard data model (discussed later) for the tags
Interoperability Level 4

Level 2: Supply Chain

Place tags on books as high in the supply chain as possible and use these tags for internal operations

- Manufacturer
- Distributor
- Book jobber
- Library

Book jobbers would like to standardize on the methodologies for programming customer tags and hopefully use one set of hardware and one set of procedures to do this task for all libraries they service.

The AFI codes for the tags will have to be programmable in the supply chain and the data on the tag would have to have different content at different stages of the supply chain.
RFID Security and Interoperability

Three security methods used today

- AFI (Application Family Identifier) based security
- EAS (Electronic Article Surveillance) bit
- Database lookup

NISO RFID Committee recommendation?

- Allow all three methods to be used
- Insist on Interoperability Requirements (AFI etc.)
- Leave security as a place of differentiation among vendors
AFI (Application Family Identifier)?

AFI is a hardware feature designed into the silicon chip on ISO 18000 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.

Programming of an ISO 15693 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 separation of applications and security implementations.
Security - AFI and Interoperability

Requirements for interoperability

- Standard AFI Code for library applications for books checked out
- Keep the AFI code unlocked
- Standard AFI Code for library applications for books checked in (checked in books can use a local – but standard – AFI code)

Required whether AFI is used for security or not.

Systems which use AFI for security should use both of the assigned codes
Systems which use EAS or database lookup for security should use the Library Industry code to avoid interference with other applications of RFID.
EDItEUR, NISO and Danish National Library Library filed a joint application for the assignment and registration for a library specific AFI code to be used for books that are checked out.

The code has been assigned!!
ISO 18000 Standards

18000-1 Part 1 – Generic Parameters for the Air Interface for Globally Accepted Frequencies
18000-2 Part 2 – Parameters for Air Interface Communications below 135 kHz
18000-3 Part 3 – Parameters for Air Interface Communications at 13.56 MHz
18000-4 Part 4 – Parameters for Air Interface Communications at 2.45 GHz
18000-5 Part 5 – Parameters for Air Interface Communications at 5.8 GHz (Withdrawn)
18000-6 Part 6 – Parameters for Air Interface Communications at 860 to 930 MHz
18000-7 Part 7 – Parameters for Air Interface Communications at 433 MHz
Scope of ISO 18000-3

“The scope of the ISO 18000-3 standard is to provide Physical Layer, Collision management System and Protocol Values for RFID Systems for Item Identification operating at 13.56 MHz in accordance with the requirements of ISO 18000-1”

Some library vendors say they are ISO 18000 or ISO 18000-1 compliant instead of the more specific ISO 18000-3 compliant, but they mean the same thing.

NISO Committee: Endorses this standard
ISO 15693

The ISO 15693 specification has three main parts:

- Physical characteristics
- Signal Interface and
- Transmission Protocol

It holds the promise of interoperability

ISO 15693 is not to be confused with ISO 15963 which is used for RFID for Item Management - Unique Identification of RF Tag (also read 15961 & 15962)

NISO Committee: Endorses this standard
There was considerable debate on how much data should be placed or even permitted on the tag. Two opposing views:

The minimalist approach … only a primary ID

The other extreme … as much on the tag as space and cost considerations would allow so that the system could function with minimum interaction with the ILS.

The NISO committee … flexibility while maintaining a fair degree of interoperability.
NISO Three Part Strategy

NISO preliminary recommendation – has 3 parts

Part 1: Content of the tag itself – **Data Model**

Part 2: **Encoding scheme** using relative OIDs

Part 3: **Logging requirements** for multiuse tags
Part 1: Data Model

Three attributes defined as mandatory

1. Primary ID
2. Use (of the tag) – stage in life cycle of tag
   - codes – 16 Manufacturer; 32 Distributor; 48 Jobber; 64 Library
3. Content Map
   - The content map is a 8 bit field indicating if a specific optional group of attributes exists on the tag or not
### Part 1: Data Model (1 of 3)

<table>
<thead>
<tr>
<th>Data Format/Lock</th>
<th>Group#</th>
<th>GroupName</th>
<th>RelPos</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Id</td>
<td>0</td>
<td>Base</td>
<td>00</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Use (stage)</td>
<td>0</td>
<td>Base</td>
<td>01</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Content Map</td>
<td>0</td>
<td>Base</td>
<td>02</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Institution</td>
<td>1</td>
<td>Owner</td>
<td>03</td>
<td>Optional</td>
</tr>
<tr>
<td>Country</td>
<td>1</td>
<td>Owner</td>
<td>04</td>
<td>Optional</td>
</tr>
<tr>
<td>Postal Code</td>
<td>1</td>
<td>Owner</td>
<td>05</td>
<td>Optional</td>
</tr>
<tr>
<td>Set Info</td>
<td>2</td>
<td>Item</td>
<td>06</td>
<td>Optional</td>
</tr>
<tr>
<td>Type</td>
<td>2</td>
<td>Item</td>
<td>07</td>
<td>Optional</td>
</tr>
<tr>
<td>Media Format</td>
<td>2</td>
<td>Item</td>
<td>08</td>
<td>Optional</td>
</tr>
<tr>
<td>Title</td>
<td>2</td>
<td>Item</td>
<td>09</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Part 1: Data Model (2 of 3)

<table>
<thead>
<tr>
<th>Data Format/Lock</th>
<th>Group#</th>
<th>GroupName</th>
<th>RelPos</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier ID</td>
<td>3</td>
<td>Supplier</td>
<td>10</td>
<td>Optional</td>
</tr>
<tr>
<td>Invoice #</td>
<td>3</td>
<td>Supplier</td>
<td>11</td>
<td>Optional</td>
</tr>
<tr>
<td>Item ID</td>
<td>3</td>
<td>Supplier</td>
<td>12</td>
<td>Optional</td>
</tr>
<tr>
<td>PO Number</td>
<td>3</td>
<td>Supplier</td>
<td>13</td>
<td>Optional</td>
</tr>
<tr>
<td>LC Class</td>
<td>4</td>
<td>Shelving</td>
<td>14</td>
<td>Optional</td>
</tr>
<tr>
<td>Dewey</td>
<td>4</td>
<td>Shelving</td>
<td>15</td>
<td>Optional</td>
</tr>
<tr>
<td>Shelf Location</td>
<td>4</td>
<td>Shelving</td>
<td>16</td>
<td>Optional</td>
</tr>
<tr>
<td>Sort bin</td>
<td>4</td>
<td>Shelving</td>
<td>17</td>
<td>Optional</td>
</tr>
<tr>
<td>Type of Usage</td>
<td>5</td>
<td>Usage</td>
<td>18</td>
<td>Optional</td>
</tr>
<tr>
<td>Usage Qualifier</td>
<td>5</td>
<td>Usage</td>
<td>19</td>
<td>Optional</td>
</tr>
<tr>
<td>Data Format/Lock</td>
<td>Group#</td>
<td>GroupName</td>
<td>RelPos</td>
<td>Category</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
<td>------------</td>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td>Institution</td>
<td>6</td>
<td>ILL Data</td>
<td>20</td>
<td>Optional</td>
</tr>
<tr>
<td>Return date</td>
<td>6</td>
<td>ILL Data</td>
<td>21</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>7</td>
<td>Future Use</td>
<td>22</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>7</td>
<td>Future use</td>
<td>23</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>7</td>
<td>Future use</td>
<td>24</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>7</td>
<td>Future use</td>
<td>25</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>8</td>
<td>Future use</td>
<td>26</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>8</td>
<td>Future use</td>
<td>27</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>8</td>
<td>Future use</td>
<td>28</td>
<td>Optional</td>
</tr>
<tr>
<td>Future use</td>
<td>8</td>
<td>Future use</td>
<td>30</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Part 2: Encoding Scheme

The Committee is still working on this section and is going to seek some expert consulting help from others.
Part 3: Logging

Logging is recommended as a system requirement. It promotes interoperability and some protection against vandalism.

The library changing the use attribute of the tag should maintain a log record of the full before and after image of the content of the tag along with the unique item identifier (UID) of the tag.

UID is the ID placed on the tag by the manufacturer and uniquely identifies the tag itself. It remains permanently on the tag.

The Log record should be maintained throughout the life cycle of the tag. Such a log record will permit the recreation of the data on the tag if the data were compromised by malfunction or by vandalism.
Migrating to Standards Based Systems

Process will be daunting; careful planning can help

Most important issue is dealing with tags

Are your tags reprogrammable?

Were they locked after being programmed?

Can your systems run in “dual” mode?

Handle old and new tags at the same time?

Can your equipment be upgraded to do so?
Migration Recommendations

Good Citizenship

- Be compliant with ISO standards
- USE officially assigned AFI code

Awareness

- Standards are public documents
- Interoperability also means greater exposure to vandalism
- Labor and other costs

Where? In what priority order? On the fly?

- At Checkin
- At Sortation system
- At ILL delivery
- At checkout
Migration Recommendations

Role of your vendor

- Monitor standards activity
- Plan, develop and offer standards based solutions
- Offer migration path with “dual” tag handling capability
  - For circulation stations
  - For self checkouts
  - For sortation systems
  - For security gates
  - For inventory systems
- Comply with data content on the tag
- Program the AFI tag and leave it unlocked
The International Scene

The Danish Data Model
The Dutch Data Model
The Australian Data Model
Copy of the data models available on the internet

International Standardization Activity

Meeting in Copenhagen

National Reps from several European countries (Denmark, Germany, Netherlands, UK, Finland, Sweden) Australia and USA.

Ongoing discussion of standards and data model

Surprised at our concern over privacy
The Timetable

Draft #3 is the current draft

Committee meets Feb 13-14 for Draft #4

Draft #5 will be sent out to selected people for comments

Final Report in May/June of 2007
VTLS RFID library management software is now RFID hardware and tag supplier independent.

www.vtls.com

Booth 1431 here
Thanks

• To the conference organizers for inviting us here
• To libraries and companies that have devoted their time to helping with this standards activities.
• To all of you for your interest in this important topic
• Do other members of the committee that are present here wish to add anything?
• Questions?