RFID

was ist RFID?

RFID steht für Radio Frequency Identification und erlaubt die berührungslose Erkennung von Medien. Gegenüber dem Einlesen von Barcodes entfällt das Suchen nach dem Etikett, mehrere Medien können als Stapel verarbeitet werden.

RFID für Buchsicherung und Selbstverbuchung

In Bibliotheken des GBV sind mehrere RFID-basierte Buchsicherungs- und Selbstverbuchungsstationen in Betrieb. Details zu beteiligten Bibliotheken sind im Bereich Selbstverbuchung zu finden.

Hier geht es um einen Überblick der eingesetzten Systeme, deren technischen Möglichkeiten und Risiken.

RFID zur Inventur

Die mit RFID bestückten Medien lassen sich beeinduckend schnell und berührungslos auf Anwesenheit überprüfen. Aspekte dabei sind:

- Sicherungszustand
- Fehlerfreies RFID Label
- Vollständigkeit mehrteiliger Medien

In der HSU wird eine Lösung entwickelt, die diese Felder abdeckt.

Weitere Anwendungsfelder sind

- Prüfung von Medien auf Arbeitstischen
- Unterstützung bei der Auswahl bzw. Durchführung von Aussonderungen

Anmerkungen zur Robustheit gegen Manipulation

Künftig muß damit gerechnet werden, daß RFID Tags auch mit Smartphones ausgelesen und auch verändert werden können. Die Möglichkeiten reichen vom Verlust des Diebstahlschutzes bis zur behebbaren oder auch endgültigen Unbrauchbarmachung des Tags.

Erste Anwendungen, mit denen auch Tags aus Bibliotheken erkannt werden, bieten etwa NFC Research Hagenberg und NXP. beide sind im Google Playstore erhältlich. NFC Research liest unter anderem das Passbild aus dem Reisepass.

Payload aka UserData

Die Datenblöcke, auf denen der bibliotheksspezifische Inhalt steht, bieten auf die Möglichkeit einer endgültigen Sperrung gegen Veränderung: *LOCK BLOCK*. Zumindest ist das Teil der Spezifikation der verwendeten Tags. Danach wäre aber eine nachträgliche Änderung beispielsweise des Medienstatus (Ausleihbar, Präsenz, Gelöscht) nicht mehr möglich. Auch genügt es nicht, alle bis auf einen Block zu sperren, weil Änderungen auch immer in der CRC (Prüfsumme) nachgeführt werden müssen, die sich bei den bekannten Implementierungen auch noch auf zwei benachbarte Blöcke verteilt.

Eine Lösung bieten hier Tags, die auch nach einem LOCK noch veränderbar bleiben, wenn ein vorher auf dem Tag hinterlegtes Passwort bekannt ist. Die Prüfung dieser Tags auf Abwärtskompatibilität in Systemen, die bislang mit ungeschützten Tags ausgestattet sind, ist an der HSU Hamburg geplant. Aus Sicherheitsgründen sollte für jedes Tag ein eigenes Passwort generiert werden, das sich aus der UID des Tags berechnen läßt.

Konkordanz UID-Barcode

Wenn ein Tag Manipulationen bzw. Zerstörungen aufweist, bleibt nur die Restaurierung. Hier kann eine Tabelle UID-Barcode (evtl auch UID-UserData) nützlich sein. Der Anbieter sollte bereits bei der Erstkonvertierung darauf verpflichtet werden, eine solche Konkordanz zu liefern. Alternativ kann jeder spätere Kontakt zum Tag genutzt werden, um eine solche Konkordanz aufzubauen.

Eine Integration der UID könnte durch Definition einer eigenen Kategorie in den Lokaldaten erfolgen, vergleichbar der EPN.

- Vorhandene Tabellen und Nachträge könnten offline eingespielt werden
- Neueinträge können auch direkt am CBS vorgenommen werden (Skripte)
- Die Abfrage erfolgt nach Indizierung performant über den OPAC bzw. Discovery
- anders als bei der EPN muß eine nachträgliche Änderung möglich sein
- Die Syntax ist leicht prüfbar: 8 Bytes in Hex (vielleicht noch uppercase)
- CBS bietet einen verbundweiten Index der UIDs

weitergehender Schutz vor Manipulation (aka Paranoia)

Um zumindest in die Lage zu kommen, Manipulationen am eigenen Bibliotheksinhalt des Tags zuverlässig zu erkennen, wäre eine kryptografische Sicherung geeignet. Die verwendete CRC (siehe Dänisches Datenmodell) wäre eine Basis, die sich mittels eines shared secret zu einem besseren Schutz ausbauen ließe.

Idee: berechne die CRC nicht immer aus dem gleichen Seed (heute: 0xffff), sondern ermittle den Startwert für jedes Tag neu. Ausgangspunkt können die beiden LSB der TagId sein, die geeignet verschlüsselt werden. Vorschläge für die Verschlüsselung:

1. shared secret - Gefahr der Kompromittierung
2. Verschlüsselungstoken - Hardwarekosten und Hardwarebindung
3. Verschlüsselungsserver - Netzwerkabhängigkeit, dafür Sicherheit verschoben auf Netzwerkauthentifizierung

Nachteil: der Schutz vor Übertragungsfehlern steht nur dem zur Verfügung, der Zugriff auf die Verschlüsselung hat - aber: wer braucht sie sonst?

Alternative: Nutze einen zusätzlichen Block mit 4 Bytes für einen kryptografischen Hash der CRC. In diesem Fall bliebe das Datenformat unangetastet.

Buchsicherung

Die Überlegungen zur Manipulationssicherheit beziehen sich - leider - nur auf die sog. *Payload*, in der die bibliotheksspezifischen Daten stehen. (siehe Dänisches Datenmodell) Die Buchsicherung hingegen wird gern mit dem sog. AFI Byte realisiert. AFI steht für Application Family Identifier und ist ursprünglich dazu gedacht, aus einer - offenbar erwarteten - Vielzahl von Tags nur die relevanten, sprich: die eigenen anzusprechen. Es lassen sich ganze Gruppen ansprechen, aber auch gezielt einzelne AFI Werte. Zur Buchsicherung wird einfach ein einzelner Wert für *gesichert* verwendet. Das Sicherungsgate spricht also gezielt nur die gesicherten Medien an und erhält von allen anderen keine Antwort. Im Hinblick auf die vergleichsweise langen Lesezeiten der verwendeten HF-RFID Tags eine besonders geeignete Methode, zeitnah auf gesicherte Medien zu reagieren.

Das AFI Byte ist Teil der Systeminformation und läßt sich sogar gesondert gegen Veränderung sperren - aber nur einmal und endgültig. Damit ist dem Bibliotheksbetrieb aber nicht gedient. Vielmehr bietet gerade diese Funktion *LOCK AFI* eine erneute Angriffsfläche. Bücher, die sich nicht mehr (ent) sichern lassen, verursachen weiteren Aufwand.

Abhilfe könnte beispielsweise der künftige Einsatz von Tags mit einer Schreibsperre (Passwort) schaffen. Ein Test mit entsprechenden Tags von TI steht noch aus. Ziel der Untersuchung wird sein, ob gesicherte Tags mit der vorhandenen Software weiterverarbeitet werden können, solange keine Schreibvorgänge erforderlich sind. Solange die vorhandenen Selbstverbucher unverändert am Start sind, gilt insbesondere, daß ausgererechnet die Buchsicherung nicht vor Manipulation geschützt werden kann.

Eine weitere Alternative könnte in einem gänzlichen Verzicht auf eine Buchsicherung durch ein Merkmal am Tag bestehen. Hierzu müßte das Gate am Ausgang jedes Medium online mit dem aktuellen Verbuchungsstand abgleichen, um ggf. zu alarmieren. Ein Auslesen des Itemcodes (aka Barcode) käme nicht mehr in Frage, weil das rund 10 mal so lange braucht, wie das Auslesen der Tag UID. Voraussetzung für diesen Weg wäre also eine Aufnahme der UID in den Datenbestand eines Mediums. Um eine ausreichend schnelle Antwort aus der Datenbank mit immerhin mehreren Millionen Medien sicherzustellen, ist eine Indizierung notwendig. Eine Aufnahme als weitere Exemplarkategorie neben dem Barcode wäre denkbar (s.o.) Die Abfrage könnte die gleiche Methode wie der DAIA Service nutzen. Ob damit eine ausreichend schnelle Antwort an das Gate möglich ist, müßte ein Versuch klären. Dieses Verfahren würde eine Manipulation der Tags zur Vermeidung eines Alarms ausschließen.

verbundweite Lesbarkeit / Einbindung Fernleihe

Stand 2011 betätigen sich eine überschaubare Zahl von GBV Bibliotheken im Bereich RFID: Die HSU, die TUHH, die Lehrerbibliothek HH - nicht zu vergessen die Hamburger Buecherhallen als Vorreiter. Aber schon ist zu erkennen, daß Verwendung des gleichen Datenmodells , sogar durch den gleichen Hersteller (hier: Lyngsoe) keineswegs bedeutet, daß die Tags gegenseitig lesbar wären. (siehe Dänisches Datenmodell) Tags, die von Bibliotheca erzeugt wurden (TUHH), unterscheiden sich etwa in der Bytefolge innerhalb der Blöcke. Selbst die Verwendung des ersten Bytes ist umstritten. Das dänische Datenmodell sieht hier vier Bits zur Unterscheidung künftiger Modellersionen vor, weitere vier Bits sind hingegen für den Status im Geschäftsgang (erfasst, (nicht) ausleihbar, gelöscht) verwendet. Bibliotheca vertauscht hier die Reihenfolge innerhalb des Bytes. Fatalerweise spielt diese Abweichung erst dann eine Rolle, wenn es um eher seltene Medien mit anderem Status als 1=ausleihbar geht, weil sich erst dann die unterschiedliche Codierung (0x21 statt 0x12) bemerkbar macht. Mit einem Test an ausleihbaren Medien ist es also nicht getan.

Es scheint dringend notwendig, künftigen Herstellern mit einer Referenzimplementierung zu "helfen", ein (zu erarbeitendes) Pflichtenheft einzuhalten. Sprich: Tags einer neuen RFID Einführung werden erst dann akzeptiert, wenn sie vom GBV - Referenzverbucher gelesen und der richtigen Bibliothek zugeordnet werden können. Eine App für NFC-fähige Smartphones gibt es bereits: den *GBV RFID Validator* im Google Play Store.

Einbindung von Lieferanten

Es ist künftig nicht auszuschließen, daß Buchhändler ihrerseits RFID einsetzen. Neu beschaffte Medien, die bereits mit einem geeigneten Tag ausgestattet sind, könnten in der Erwerbung einfacher einer Bestellung zugeodnet werden. Idealerweise ist das Tag im eigenen Hause weiterverwendbar.

Leitlinien

aus dem Vortrag von Ulrike Verch 2007 [1]

```
-keine bibliographischen oder persönlichen Angaben auf  RFID-Chips speichern
-Verschlüsselung oder Authentifizierungsmechnismen
-deutliche Kennzeichnung der Lesegeräte oder  Kennzeichnung des Bibliotheksausweises mit „Funk-Logo“
-regelmäßige Wartung der Lesegeräte und Überprüfung  der Sicherheitsstandards
-Informationsblätter zu RFID bereithalten
-FAQs erarbeiten
-RFID-Beauftragten der Bibliothek ernennen
-regelmäßige Fortbildungen des Personals zu RFID
-Zusammenarbeit mit Personalrat und  Datenschutzbeauftragten
```

Was ist davon bereits umgesetzt oder schon überholt?

Hardware

Tagsys

Für Lesegeräte der Firma Tagsys liegt eine quelloffene Implementierung eines Desktoplesers vor, der eine besonders schnelle Visualisierung der "sichtbaren" Medien mit Sicherungsstatus bietet. Unterstützt werden - dank Java - Mac, Linux und Windows. Anfragen gern an Ulrich Hahn, HSU .

Feig

- bitte ergänzen -

Glossar

- AFI - Application Family Identifier, ein Byte, mit dem sich gezielt einzelne Tags ansprechen lassen, während die anderen schweigen.
- DSFID - Byte zur Klassifizierung des Taginhalts (nicht verwendet)
- EAS - Electronic Article Survey, Sicherung, die eher im Einzelhandel Verwendung findet
- SystemData - beschreiben die Eigenschaften des Tags, enthält u.a. die UID und die Anzahl der Blöcke auf dem Tag

- Dänisches Datenmodell - fixed-length-Format, das auf 32 Byte (8 Blöcke à 4 Byte) wesentliche Daten zu Medium und Bibliothek enthält
- NFC - Near Field Communication (aka RFID), so heißt RFID für Smartphones
- NDEF - NFC Data Exchange Format. Erlaubt mehrere NDEF Records auf einem Tag. NFC und NDEF sind Spezifikationen des NFC Forums
- NDEF Record - Eine Nachrichteneinheit mit bekanntem Typ z.B. eine URL, eine VCard, ein Text, eine formatierte Nachricht (hier könnte auch das Dänische Datenmodell stehen) https://code.google.com/p/ndef-tools-for-android/
- UID - unveränderliches Kennzeichen eines Tags, besteht aus 8 Byte, und bietet einen ausreichend großen Adressraum von 10^19 Einheiten. Die ersten Bytes geben einen Hinweis auf den Hersteller. Amtliche Ausweise wie der Reisepass oder aktuelle Personalausweis verwenden übrigens für jede Verbindung eine neue UID, sind also - anders als unsere Tags - nicht allein an der UID zu identifizieren.
- UserData - frei beschreibbarer Bereich (Dänisches Datenmodell)

Links

- Deutscher Bibliotheksverband zu RFID

- 3M
  - 3M Library RFID Solutions
  - 3M RFID Case Studies & Whitepapers
  - 3M again (RFID 301 deutsch)

- NFC Arbeitsgruppe beim W3C
- nfc-tools.org
- nearfieldcommunication.org
- Anbieterübersicht im B.I.T. Wiki (leider veraltet --Hahn (Diskussion) 13:30, 24. Sep. 2014 (CEST))

- Berühren statt klicken - Artikel aus ix 03/13 zum Stand der Dinge bei NFC

- NDEF Spezifikation

Anbieter

- Nedap library solutions
- Bibliotheca RFID
- Lyngsoe / vorm. FKI Logistex