Book Industry Communication Advisory on EU Mandate M/436 on RFID Privacy Part 2 (Version 3) EN 16571

Disclaimer: BIC is not a legal advisor and cannot give legal advice. Libraries and all other affected organisations should seek their own legal advice to enable them to fully comply with UK Law.

This advisory deals with the second part of the EU Mandate M/436 on Privacy in RFID implementations: EN 16571. (Note that there is a first part dealing with the requirements of EN 16570.)

1. Who is this advisory for?

This advisory is intended for librarians, library stock suppliers, organisations which undertake RFID tagging on behalf of libraries, RFID Systems vendors and LMS vendors.

2. Introduction

This advisory details BIC's advice for libraries wishing to understand EN 16571. It is important to realise that, at the time of writing (April 2015), this is not yet law and is not binding on UK library services or their suppliers. The evolution of EU mandates into UK law is, however, a well-established process and this advisory should be read as an early warning of probable legislation in the future. The purpose of this advisory is to enable libraries to get a head start in understanding the requirements of M/436 and to be ready to take action in the event that its provisions are enacted in UK law. Note that the exact requirements implemented in UK law may differ from those described in this guide. In this event, further clarification will be made available by BIC.

Two standards, EN 16570 and EN 16571 have been developed to implement the recommendations of the Mandate. The first of these (EN 16570) is basically about library signage and alerting users to the presence of RFID (BIC Advisory on EN 16570 refers). The second (EN 16571) requires that the library undertakes a Privacy Impact Assessment (PIA) to assess the risk to privacy from using RFID and the steps that the library has taken to mitigate this risk. This requirement could have a significant impact on libraries and their suppliers in terms of cost and the processes needed to mitigate perceived risks to privacy.

3. What is EN 16571 about?

EU citizens have a right to be protected from any invasion of their privacy. Library use of RFID has been identified as one possible area with privacy concerns because:

- It can be used to track physical items, and thus individuals with those items (e.g. RFID tagged books) in their possession might possibly have their movements tracked.
- It may be possible for an RFID scanner to read the tags on library books in the possession of a library user, and for example, to identify certain interests, patterns of behaviour etc. that would constitute an invasion of that individual's privacy.
- Although library tags rarely contain personal information, the tags can be connected to an RFID interrogator (e.g. a kiosk) and this links to the LMS which may contain personal information e.g. name, address etc.

4. What the mandate requires

1. ***RFID operators must undertake a privacy impact assessment (PIA) process to establish the level of risk and what can be done to mitigate the risk***

An RFID operator is any organisation responsible for RFID. This obviously includes libraries that deploy RFID but it may also include organisations such as library stock suppliers who encode data on RFID tags. Note that the PIA to be undertaken by stock suppliers would probably be at a lower level as there may be no privacy risk in supplying tagged books to libraries as a business to business supply. However, the mandate insists that if a supplier encodes an RFID tag on a product, and supplies it to a non-RFID capable library, and this book is then issued to a customer, then the stock supplier not the library is deemed to be the operator and so would have to undertake the higher level of impact assessment. Under these rules there may be other organisations that could be identified as operators e.g. 3rd party tagging organisations and RFID vendors.

It will be necessary for libraries and their suppliers to consider this requirement and decide for themselves with the appropriate legal advice who is an operator and therefore who must undertake a PIA.

In addition there is a significant role for both RFID Vendors and LMS Vendors envisaged in EN 16571. Although they may not have to go through the whole process, they may be expected to contribute detailed information about their systems (Capability Statements).

2. ***The first step of the PIA is to produce an RFID Functional Statement***

This is an overview of the RFID Application in the organisation. The Functional Statement gives basic information such as the legal name and location of the organisation, the person responsible for the Functional Statement, the purpose of the RFID application(s), geographical scope, types of users/individuals impacted by RFID application and the list of encoded data elements used.

Producing this Functional Statement may in time be made easier by utilising:

- Templates produced by industry bodies, consortia etc.
- Capability statements produced by RFID Vendors

RFID Capability Statements would describe the technical details of an RFID application such as the standard functionality, capabilities, air interface frequencies, standard data encoded on tags, read ranges, power consumption etc. together with any privacy countermeasure capabilities.

Operators can use this information to inform their RFID Functional Statement. Where their application differs from the standard application e.g. additional data encoded on the tag, this would need to be added to the Functional Statement.

If the initial analysis and the functional statement documents that no RFID tagged object is in the possession of, or associated with, an individual, then the PIA process ends there. If the tagged object is in the possession of, or associated with, an individual, (as is very likely with RFID tagged library books) then the process continues as follows:

3. ***Privacy Impact Assessment Report***

This is the main deliverable which describes the assessment in detail. The process starts with looking at the various elements. Note that EN 16571 goes into exhaustive detail and this is only a

high level summary:

Asset:	An RFID tagged book is an example of an asset.
Threat:	Unauthorised tag reading, tracking, behavioural profiling, unauthorised modification.
Vulnerability:	A way of scoring threats based on how likely/unlikely they are over time.
Data Type:	The information stored on tags is given a risk factor e.g. personal information scores more highly than product information.
Risk:	Quantified level of risk deduced by looking at any threats associated with each asset and over time influenced by known vulnerabilities.
Countermeasure:	What can be done to protect RFID applications such as tag encryption, password protection, tamper proof tags etc.
Residual risk:	Level of risk remaining after countermeasures.
Threshold:	The current level of risk which is deemed acceptable for now.

This is an established risk assessment process and it involves scoring each element, ending up with a total which shows the level of risk. EN 16571 contains tables of values for each asset, threat, data type etc. and these values are to be fed into a table to arrive at the risk result. Countermeasures are also listed and these can reduce the risk level. There is very little complicated calculation, just looking up values in tables, adding up risk factors and subtracting countermeasures.

The number of threats/data types to be analysed (and therefore the workload) reduces with the size of the organisation. Organisations are classified into three sizes in order to reduce the burden of the process on smaller enterprises:

Medium:	<250 employees, Turnover < €50m, No of Data types: 6, No of threats: 4.
Small:	<50 employees, Turnover < €10m, No of Data types: 4, No of threats: 3.
Micro:	<10 employees, Turnover < €2m, No of Data types: 2, No of threats: 2.

4. Privacy Impact Assessment Summary

The final step is to write a summary of this report which is the information that must be made available to library users and EU citizens on demand (as specified in EN 16570). Clearly this will not contain all the detailed information about threats but it will describe the RFID application, what it is used for and any privacy issues that the individual needs to be made aware of.

EN 16571 assumes that when RFID Privacy becomes UK law, an organisation such as the Data Protection Agency (DPA), will be monitoring compliance with the process and in order to be compliant, the organisation (e.g. library) will be expected to deposit the functional statement, report and summary with the DPA authority.

EN 16571 also envisages the existence of a Registration Authority which will store the capability statements supplied by RFID vendors and make them available to operators to help fill in their functional statements and privacy impact reports. At the time of writing the Registration Authority is not known and it is unclear how this authority will be set up, funded and managed. RFID Vendors would have to be persuaded to contribute capability statements for their standard products to this authority. The idea is to reduce the amount of work and duplication involved in the lengthy privacy impact assessment process

The PIA process has been developed for all RFID applications in all industries. Some industries, e.g. retail have generally lower risk because RFID tags can be switched off (at the till), some, e.g. RFID tagging of blood samples, may have very high risk because they may contain personal information and even DNA data. Libraries constitute quite a high risk because tags are not switched off on exit from a library (because self-return is required later). Although most RFID tags in libraries don't contain personal data, the tag may be linked to a database which does contain personal data. This means that library RFID operators will need to undertake the full PIA process and the overall security of the organisation's network, LMS etc, will have a bearing on their risk level.

5. BIC's general advice

In spite of all the above, BIC's general advice is not to panic:

1. EN 16571 is not yet in UK law and may be only partially implemented.
2. Size considerations will reduce the onus on (medium), small and micro enterprises
3. Industry bodies may develop templates which will do a lot of the work
4. Many libraries will have identical risks and information can be shared
5. RFID Vendors may contribute capability statements on their applications

To start with at least, this process is not pass or fail, but it is an exercise in analysing privacy and security for the organisation and its users. This awareness combined with regular reviews and on-going vigilance and the development of additional countermeasures over time, will be of benefit to the library industry. However, the library industry needs to be aware in advance of this requirement and any costs/issues associated with it. It might be necessary to look at central funding for libraries in the event that they are expected to implement EN 16570 and EN 16571 in full.

6. Specific advice for library organisations

Libraries: Keep aware of the Privacy issue. Monitor the BIC website at www.bic.org.uk

Library Stock Suppliers: Consider whether EN 16571 defines your organisation as an operator and whether you will have to undergo the full PIA process.

RFID Vendors: Consider the implications of producing Capability Statements for each of your applications. Also be aware that EN 16571 covers the interface with the LMS. Countermeasures may become a source of product differentiation and thus competitive advantage.

LMS Vendors: The privacy (and security) envisaged in the scope of EN 16571 covers the LMS application where personal data is stored. The RFID interrogator may link to the LMS via different protocols and different media e.g. WIFI etc. This constitutes an area of risk and if EN 16571 is implemented in the UK, libraries will be coming to LMS Vendors as well as RFID vendors to secure these interfaces and look for countermeasures to any privacy risks.