RFID Privacy in Libraries – The State of Play

What is this about?

The recent publication of the European Standard: EN 16571: 2014 *Information technology - RFID privacy impact assessment process* adds a new responsibility for libraries and the privacy of their patrons. EN 16571 is applicable in 33 European countries[1] and published as a national standard with identical text, sometimes translated into the preferred language of the standards body. But as the standard is about addressing good governance, then any library and any library supplier anywhere in the world should give it consideration. The risks to personal privacy do not stop at the boundaries of Europe.

The approach adopted in EN 16571 is very different from other PIA processes. It is focussed on RFID, which the European Commission has ruled includes smart card and NFC. It addresses the privacy issues (encoded data, threats, vulnerabilities and countermeasures) based on the specific protocols, tags and reader products being used in an RFID application. As such it enables accurate and comparable PIA reports to be produced by organisations that are defined as *RFID operators*. A library that uses RFID is an *operator*, but so too are others as we discuss later.

The standard is seen by the European Commission as one of the steps towards the new EU **General Data Protection Regulation**. This has one key requirement that impacts RFID:

> **Data protection first, not an afterthought:** 'Privacy by design' and 'privacy by default' will also become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm.

The **Regulation** is an interesting legal device in the European Union. When it is approved, and this is expected in 2015, it becomes common law across all EU member states, and all new candidate state will also have to adopt the law on accession to the EU.

Libraries can take different approaches to EN 16571, from:

- hoping that it goes away (very unlikely)
- ignoring it for as long as possible
- being compared unfavourably with other libraries that undertake the RFID privacy impact assessment (PIA) and display the necessary signage
- showing good governance and beginning to address the issues
- being required by some European national Data Protection Authorities to undertake the RFID PIA

We have been working on RFID privacy issues for nearly 10 years and heavily involved with others including CNRFID, the French National RFID Center, in developing EN 16571. We know the standard. We know that it requires an understanding of RFID technology that a number of libraries might not possess. So there is another option. CNRFID has partnered with Convergent Software Ltd to develop and market software that complies with EN 16571. This will simplify the task of organisations using RFID to develop their RFID privacy

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

impact assessment (PIA) report and comply with the standard. If you visit http://rfid-pia-en16571.eu/ you can learn more.

In the rest of this document, we provide advice about the types of library application that fall within the scope of EN 16571 and about the role of various stakeholders. We also address some basic points about notification.

What are the key RFID library applications?

The most obvious library application is any function associated with **circulation control**. This covers self-checkout, returns, the security gates, staff work stations, book drops and internal stock control. The key point to understand is that the loan items that carry RFID tags are the ones that interact with the patrons. Within the library, there is not too much risk of loss of privacy, this increases when a loan item is removed from the library. This is what EN 16571 calls the *uncontrolled domain*.

While a library might ensure that obvious personal information is not encoded on the RFID tag, the very fact that the bar code number (primary item identifier, as defined in ISO 28560) is encoded and even the unique chip identifier do make a patron identifiable. In some countries there is concern that identifiers like the ISBN makes the person identifiable, but all it does is provide a source for a search on the type of book being carried by a patron.

Remember that RFID Privacy needs to address any radio frequency protocol. This means that if the **membership card** uses some form of radio frequency, then it too is considered to be an RFID application. Again, for most RFID protocols to work, there is a requirement to uniquely identify a membership card and this normally calls for a unique chip ID to be used. That, combined with a membership ID code, adds to the privacy mosaic. Encoding anything explicit like a patron's name or phone number adds to the privacy risks.

Depending on the type of library, library staff might also be issued with **identification badges**. Where these are RFID enabled, then a privacy impact assessment should be undertaken.

In recent years, there has been a rapid increase in the use of contactless payment in Europe and other countries. It is now rapidly emerging in the United States since laws were introduced to phase out magnetic stripe cards. Such **contactless payment cards and tokens** should also be the subject of a privacy impact assessment.

The introduction of **near field communication (NFC)** has opened up opportunities for libraries. The very fact that smart phones that are enabled with NFC can support the function of emulating an RFID tag or card, also brings them within the realm of requiring an RFID PIA if they are used as part of the system by patrons.

From all of the above, it should be clear that libraries that do not use RFID for circulation control might well require to undertake an RFID privacy impact assessment, because of other uses that are made of the technology within the library.

What stakeholders have a responsibility for RFID privacy?

It should be obvious from the list of applications that the **library itself** and its owning authority have a responsibility for ensuring that RFID privacy is achieved. The PIA process requires a risk assessment to be undertaken, which should help with future plans to improve patron privacy. There are some interesting variations on a theme. University and hospital teaching libraries might well use staff access control badges, not only for the library staff but also for the *patrons* who might be staff or students. Some public libraries have membership cards issued by the owning authority, which provides the holder of the card with a much

wider set of privileges and functions than just that of being a library patron. In the cases where such cards are used, it might be appropriate for the owning authority to undertake the privacy impact assessment based on all the functions supported by the cards with the library focusing more on the circulation control aspects. School libraries that use RFID might need to take even greater care and undertake a RFID PIA.

A fact that is not widely appreciated is that those who encode tags and smart cards also have a responsibility as RFID operators. So this would apply to **book suppliers and jobbers, conversion agents**, and any organisation that provides encoding services other than the library itself. Encoding tags on loan items is likely to require a very low level of privacy impact assessment, but those that encode RFID membership cards that require access to any personal information probably need to undertake the highest level of privacy impact assessment.

This might be a useful place to provide some information about the breadth and scope of the RFID privacy impact assessment process. The basic objective is to take into account the data on the RFID tag, the threats to which that data is exposed and associated vulnerabilities. This produces what is known as the initial risk assessment. EN 16571 specifies some quite precise rules to achieve this. Depending on the nature of the data encoded on the RFID tag or card, rules determine the level of privacy impact assessment required. The highest of three levels (level 3) is where personal identifiable data is on the RFID tag. Under existing European Data Protection law, the definition of what is personally identifiable is quite extensive. If there is no personal identifiable data or personal behaviour data on the RFID tag, but this is on the application, then a level 2 PIA is required. Only if nothing like this exists on the tag and the application, can a PIA be considered the lowest level 1 category.

Depending on the determined PIA level, different aspects of the RFID application need to be considered. With the highest level, it is end-to-end from the RFID tag to the application layer.

The **RFID system providers** do not have to undertake a privacy impact assessment, unless they perform one of the functions immediately above. However, they can significantly simplify the work for libraries by providing information about the tags, RFID tag chips and interrogators (readers) that are being used. There is a Registration Authority where details of products can be provided. Details in English and French are available here:

http://www.centrenational-rfid.com/registration-authority-article-137-gb-ruid-202.html

http://www.centrenational-rfid.com/autorite-denregistrement-article-137-fr-ruid-17.html

In some cases, a library might purchase tags or even RFID equipment directly. In such cases, the **suppliers of the RFID equipment** (tags, printer encoders and reading devices) have a responsibility to provide information either directly to the library or to register details with the Registration Authority.

Providers of **library management systems** (or integrated library systems, depending on where you are based) also have a responsibility. Although the communication protocols such as SIP2 are fairly restricted in what data elements from ISO 28560-1 are supported, the LMS/ILS systems do contain a lot of information about the loan items and the patrons. Any RFID-enabled library will need to ensure that it understands the nature of information that is held on the LMS/ILS. It would obviously make even more sense if that aspect of the privacy impact assessment was based on information provided by the suppliers.

Some interesting development that have taken place in the past few years where some functions of the LMS/ILS are supported by cloud computing, rather than an in-house database. In this case, the European

Union lays down quite strict rules under existing laws for the transfer of data beyond European boundaries. This not only applies to member states within the EU, but other countries within Europe. There are provisions for accepting cloud-based services and other facilities being hosted outside of Europe, but these are fairly strict and somewhat limited in function.

A more recent development is where the LMS/ILS supports a web-based or cloud-based OPAC that can be accessed via a smart phone. If there is any use of NFC or RFID tags then this too falls within the realms of RFID privacy.

Notifying the presence of RFID

A keynote on the Commission's Recommendation on RFID (2009) was the requirement for transparency. This has been carried forward into the new Data Protection and Privacy regulation. As is usual with legal documents, there are a number of preambles:

> (46) "The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand and that clear and plain language be used..."
>
> (48) "The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes..."

The original Recommendation had this more explicit requirement about "Information and transparency on RFID use". Here is the whole of Clauses 7 and 8:

> 7. Without prejudice to the obligations of data controllers, in accordance with Directives 95/46/EC and 2002/58/EC, Member States should ensure that operators develop and publish a concise, accurate and easy to understand information policy for each of their applications. The policy should at least include:
>
> (a) the identity and address of the operators;
>
> (b) the purpose of the application;
>
> (c) what data are to be processed by the application, in particular if personal data will be processed, and whether the location of tags will be monitored;
>
> (d) a summary of the privacy and data protection impact assessment;
>
> (e) the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks.
>
> 8. Member States should ensure that operators take steps to inform individuals of the presence of readers on the basis of a common European sign, developed by European standardisation organisations, with the support of concerned stakeholders. The sign should include the identity of the operator and a point of contact for individuals to obtain the information policy for the application.

Therefore, in parallel to EN 16571, there is a requirement for an RFID operator to display signage that explains that RFID data capture is in operation. This signage should give basic information about the RFID operation and display the RFID emblem.

As this shows there is also a requirement for the sign to point to the source of a publicly available privacy impact assessment summary. The PIA summary provides basic details about the RFID operation, the

residual risk, and any additional countermeasures that, in the case of a library, the patron can take into account.

There is even an interpretation that the emblem and very basic information shall appear on every item that carries an RFID tag. As this is intended to achieve continual awareness, we think that there are other better ways of doing this that might be acceptable.

Summary

As we set out at the beginning of this paper, a library has many options on whether it takes actions in preparation of the new Regulation or, at the other extreme, ignores everything until the eleventh hour. There is also the possibility that the Data Protection Authorities will take slightly different views to the time scale for implementation. However, do not assume a laisser-faire attitude. All the heads of the European DPAs are members of the Article 29 Working Party [Article 29 is the relevant article in the 1995 Data Protection Directive calling for legal oversight]. The Article 29 Working Party has already commented on its expectations for an RFID PIA Framework[2]: That Framework is fully supported by the processes defined in EN 16571.

> The Working Party endorses the Revised Framework submitted on January 12, 2011. This framework shall take effect no later than 6 months after the publication of this opinion.
>
> A PIA is a tool designed to promote "privacy by design", better information to individuals as well as transparency and dialogue with competent authorities. Consequently, since some RFID Applications will be implemented in several member states, it is important that PIA reports are translated and made available to competent authorities in their national language.
>
> The Working Party will continue to support future dialogue with the industry, with regards to providing enhancements and clarifications in the structure and implementation of the RFID PIA Framework, as informed by experience and feedback from all stakeholders.

Already, organisations have taken heed of both the Framework and EN 16571. Some RFID operators are already displaying the emblem, even to the item level. Major RFID product manufacturers are providing information about the privacy capability features of their products.

Convergent Software Limited will provide library-specific information on our website and in our newsletters. More generic information will continue to be provided on the CNRFID-CSL website http://rfid-pia-en16571.eu/.

Because there might be some issues that need to be addressed in a particular manner, we will be happy to receive any enquiries addressed to: rfid-pia@convergent-software.co.uk. We will then be able to discuss issues on a bi-lateral basis.

[2] Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm