Introduction

This paper explains three related Commission RFID initiatives and invites comments on document 3, the public consultation document, by 6 September 2010. The table of draft comments that follow are based on the that document. It is not essential to read the first two documents described below.

1. Commission Recommendation of 12 May 2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio Frequency Identification

http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

A Recommendation from the Commission requires Member States to take some action and is, effectively, one step before a legally binding Directive that is taken into law by all Member States. As such, it is a preview of the direction of potential future legislation. Within a year of publication of the Recommendation a number of actions should have been taken by the Member States to ensure that operators (including libraries):

- develop and publish a concise, accurate and easy to understand information policy for each of their applications.
- provide a summary of the privacy and data protection impact assessment carried out on the RFID application.
- inform individuals of the presence of readers on the basis of a common European sign.

2. European Commission Standardisation Mandate M436

http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/m436EN2.pdf

This Mandate was issued to the European Standards Organisation (ESOs) to develop standards to support the Recommendation. The Mandate calls for two phases of work: a research process by a group of experts, followed by specific standardisation by the European Standards Organisations (CEN, CENELEC and ETSI). Phase 1 started work in March 2010 and has delivered a public consultation document (see below). Phase 2 is likely to begin early in 2011, which will result in a set of standards that formalise, for example, signage, privacy impact assessment and other features.

3. Radio Frequency Identification (RFID): co-ordinated ESO Response to Phase 1of EU Mandate M436

http://www.cen.eu/cen/Sectors/Sectors/ISSS/Documents/RFID-DTR07044v006-draft-for-public-comments.pdf

This is the public consultation document on which the library community and others are invited to comment. The draft comments in the following table refer to this document. Your suggested additions and changes should be sent to Brian Green, brian@editeur.org by Monday 6 September. (We suggest that you use “track changes” if your revisions are extensive.) They will be reviewed, collated and submitted by EDItEUR as a single document on behalf of the sector. N.B. We have not included purely editorial comments as these will be made separately.

Clause (e. g. 3.1)	Para-graph/ Figure/ Table (e. g. Table 1)	Type of com-ment (e. g. ed)	Comments: Justification for change	Text of proposed change
5.1	Page 16		**Proposed Comment:** Library customers are aware of the presence of the technology because they themselves are involved with self-service transactions for checkout and returns. There is no requirement for logos on the individual loan items.	**Proposed Text:** Add the following text: "There are some circumstances, for example in library self checking systems, where the process performed by the customer makes them fully aware of RFID."
5.2	Page 16		**Proposed Comment:** The RFID tag on a library book, and other loan items, is used exclusively for circulation control and internal stock control.	
5.3	Page 17		**Proposed Comment:** This approach to deactivation is strongly opposed by the library community. The rights to deactivate should only be possible if the consumer legally owns the item, and this is not the case with library books. The current type of tag used in the library community does not support any form of deactivation and reactivation, and this text is ignoring the realities of the technology without offering any solutions.	
6.7	Page 20 penultimate para	te	**Proposed Comment:** The text "For the purposes of RFID it is recommended that where explicit personal data is deployed on a tag that only those devices capable of supporting encrypted storage or transmission of data should be deployed." Is currently impossible with existing technology. The report (a) does not acknowledge this and (b) provides no advice or recommendation to address this. The solution needs to address the migration of existing applications, and not just be presented as the 'next good thing'. Additionally this is a bad place to 'bury' a significant recommendation.	**Proposed Text:** Change the text to "Given that most current RFID technology does not yet support encrypted storage or transmission of data, it is recommended that standards and products are developed to support this feature. Such products need to take into the basic operational requirements of applications. When such technological solutions are available, explicit personal data should be store in an encrypted format."
6.7	Table 1 (pages 21 to 23)		**Proposed Comment:** No comments will be submitted on the table, based on the assumption that all these points are covered later in the discussions on privacy.	
7.2	Page 24, 1st para under Note		**Proposed Comment:** The use of the word "intent" implies a basic design requirement. This is certainly not the case for library systems and creates a completely distorted position for the general reader.	**Proposed Text:** The first sentence should simply read "A secondary privacy concern is that there is a possible capability of the system to track individuals".
7.2	Page 24, 2nd para under Note		**Proposed Comment:** Given that many RFID tag technologies require a unique chip ID for anti-collision purposes, this paragraph fails to address the reality of the present technology and its deployment.	

7.2.1	Page 27 last two paras		**Proposed Comment:** These two paragraphs give the impression that asserted data is wrong and requires additional privacy enhancing techniques. In a library situation, there is a requirement to assert the time of the transaction and the person borrowing the book for circulation control, liability in case of loss, return reminders, and fines. There is no need for privacy enhancing techniques as all of these features are part of the base Data Protection assessment and requirement for the library management system. In addition, none of this is directly associated with RFID technology, but applies equally when only bar code technology is used to identify the loan item or even when no automatic data capture technology is used. The tone of these two paragraphs imply that something is naturally missing and not considered, when the opposite is the case.	
7.3.1	Page 29, Table 3 DPP0-1		**Proposed Comment:** As previously stated " mechanisms to provide disablement or kill functionalities" are the exact opposite of what is required for a library system. This text needs to be changed to reflect many types of RFID application. On present reading it implies that libraries are non-compliant with DPP requirements.	
7.3.1	Page 30, Table 3 DPP0-4		**Proposed Comment:** The statement in the paragraph beginning "Deployers…"in (ii) about an RFID tag being almost invisible is completely misleading. An RFID tag consists of a chip, which is typically millimetres square and, most importantly for size, an antenna. To achieve any read range, the tag must have an antenna of a reasonable size, almost irrespective of any RFID technology. Therefore, delete this misleading statement. In the same paragraph in (iii), the requirements of "visual indication of activation" is not strictly possible. Also, "temporal disabler tag physical remover feature etc" are as has been stated more than once in our comments, a feature that makes the operation of an RFID library system absolutely impossible. This comment should be removed from this general section because multiple use tags are quite common in many RFID applications.	
7.3.1	Page 33, Table 3 DPP0-10 Para beginning "Tag content rectification"		**Proposed Comment:** For many RFID technologies, including that used in the library community, it is impossible to erase and scramble the chip's serial number, because this is essential for communications. Erasing the primary item identifier will also destroy all functionality for a library system. Even 'scrambling' this code will have serious implications because of the necessary integration of RFID with bar code data capture and the pre-existing code structures on the library management system. All the text in this paragraph needs to be completely revised to address real systems, and possibly even delete much of the content.	

7.3.1	Page 33, Table 3 DPP0-10 Para beginning "Tag content deletion"		**Proposed Comment:** The text "deployers of RFID technology should take into account that individually selecting the removal of the tag should not be penalised in any way" is in direct conflict with the ownership of the loan item. This text implies that anyone borrowing a library book can deface it without any form of penalty or punishment. The text needs to be completely removed or qualified in a way that implies ownership of the item. The library community is opposed to the first three of the listed solutions, as they will destroy the basic functionality of a tag being re-used. We have mentioned a number of times that the report fails to take into consideration the fact that the tags are owned by one organisation and are only temporarily held by an individual.	
7.3.2	Table 4 SO-4 & SO-5		**Proposed Comment:** The report contradicts itself, claiming elsewhere that the tag is openly vulnerable to access, so the terms "tagged item, tag," should be removed from these two statements.	
7.3.2	Table 4 SO-7		**Proposed Comment:** The library community agrees with this statement, but this contradicts what has been said earlier about data protection. Probably one way to correct the data protection "rights" of an individual to delete or remove data is for this to be authorised by law or by the system. This would make a significant improvement for libraries because changing data by any member or other person would be deemed to be unauthorised. Therefore, review all the approaches in 6.7 (Table 1) and 7.3.1 (Table 3) that seem to point to all RFID applications having an over-simplified monolithic structure where the ownership of the tag transfers on the first instant to the citizen holding the tagged item. This does not apply to library books, library membership cards, travel cards, passports, and many other applications.	
8.3	Page 39 Table 5		**Proposed Comment:** We were surprised to find that this table is identical to one in Annex C. This table should be deleted and a forward reference made to the relevant annex. On this basis, we will reserve our comments until we review Annex C.	
8.4.1	2nd para		**Proposed Comment:** The two sentences " This is made possible if a tag cannot distinguish between authorized and unauthorized interrogators. To the tag, a interrogator is a interrogator." seem to contradict each other when considered against almost all current RFID technology. There are no authorisation procedures, so the second sentence is right. Is the first sentence redundant, or is a recommendation being implied? If this is a recommendation what cost justifications are put forward. RFID has been implemented for many years on the basis that anyone with an interrogator can read the tag. In the library community this is leading to new applications using different devices but based on the same tag - therefore same basic investment. This would also impact adversely on inter-library loans.	
8.4	Table 6 (page 42)		**Proposed Comment:** As this table has no explanatory text and seems to be a summary of more detailed tables in Annex D, we will be making our comments against that annex. We suggest that there is a forward reference to the annex.	

9.4.2	2nd para		**Proposed Comment:** The library community agrees that the domain and sector-specific PIA guidance is required. However, in order to do this user communities need PIA methodologies to take into account the different features of the different technologies.	**Proposed text:** The first bullet should be extended to read as follows: "Standard RFID-specific PIA methodologies, built around the functional capabilities and physical characteristics of the major RFID standards air interface protocols." We also suggest a second (new) bullet: "Standard RFID-specific PIA methodologies built around the RFID system architecture."
9.4.3	Page 47 5th bullet		**Proposed Comment:** The library community is firmly of the opinion that one common PIA can be produced based on ISO/IEC 28560 with some informative annexes on proprietary systems. This will provide a pro forma on which individual libraries might only need to select specific operational options that are common to some but not all other libraries. For example, operational differences apply to; • which data model is being used, • the security systems used to minimise theft • the technical characteristics of the membership cards.	
9.4.3	Page 48 2nd bullet		**Proposed Comment:** The library community has some reservations about a PIA audit process. This looks like the creation of a new class of "inspectors" that seem to specialise in PIA audits as opposed to understanding the sector (see next comment).	
9.4.3	Page 48 3rd bullet		**Proposed Comment:** We fully support accountability to an independent supervisory body such as the national Data Protection Authority. The advantage of this is that the generic library sector PIA could be approved by the DPA, with individual library authorities then being required to register their reports. This would then eliminate the need for this new breed of PIA audit inspectors.	
9.4.3	Page 48 4th bullet		**Proposed Comment:** If the PIAs are registered with the Data Protection Authority (as we propose above), there seems to be no advantage in making them publicly available. What the DPA might do, is keep a list of registered PIAs so that individuals can check whether the RFID implementation is known to the DPA.	
9.4.4.3	Tables 7 & 8 (pages 50 to 54)		**Proposed Comment:** These tables are extremely confusing. From the layout, we are not sure whether the gaps between some of the rows are intentional or accidental, in which case is there missing content? Additional poor editing makes it difficult to follow the thread of these points. There are references to Annex A, but because the references do not exist and nothing in that annex matches. The same applies to Clause 5 which generally consists of a few lines yet seems to figure quite significantly. If we knew how to interpret these tables, we might make comments but the presentation is far from helpful.	

9.4.4.3	Page 54 Last para		**Proposed Comment:** This paragraph is completely confusing, and we had to read it more than once to establish that Table 5 really means Table 9, and that Tables 3 and 4 really mean Tables 7 and 8. Again, there is a reference to Annex A.2, which does not exist.	
9.4.4.3	Table 9 (pages 55 & 56)		**Proposed Comment:** The library community is concerned about the inclusion of some of the category/issue for the following reasons: • Issues like data mining and profiling are not necessarily associated with RFID. • Smart technologies, as mentioned before, have – to some extent – been excluded from the scope of this report yet are brought up here. • Internet of Things/ambient intelligence is something that is beyond the current scope and capability of RFID. • Corporate espionage is really about what the report calls back-end systems and not about RFID. Therefore, we consider that a significant "health warning" should be associated with this table indicating that its content is rather speculative with respect to RFID and only needs to be considered in an RFID privacy impact assessment **if and when the technology to support these issues actually exists.**	
12.1.2	Page 72 1st para		**Proposed Comment:** In the third line the value 0.02% and 500 times are shown as equivalent. 0.02% relates to 5000. Which is correct?	
12.1.2	Page 72, 2nd and 3rd paras		**Proposed Comment:** The last sentence of the second paragraph and all of the third paragraph is the first significant acknowledgement (three quarters of the way through the report) of the issues that concern established implementations of RFID as in the library community. The installed base of libraries already exceeds market penetration of most other sectors. In addition, the lifespan of typical RFID stock averages 8 years. So if a new technology was to be introduced today, it would take until 2018 – at the very earliest – before all the old technology was replaced. In reality, the inertia created by management and investment decisions would mean that the present technology will probably be in use for at least 12 years from the availability of any new technology. In addition, any new technology needs to meet the functionality required for a library RFID system. As an example, the current 16-bit random number used for anti-collision in 18000-6 Type C and proposed for 18000-3 Mode 3 results in 65536 different unambiguous codes. To put matters into perspective, the Rotterdam Library has 1.2 million items, so each randomised item code would occur 18 times on average. The library community will need convincing that new technology is fit for purpose in a library application.	

12.2.2	Table 10, Gap 1.1		**Proposed Comment:** To use one of the terms in the report, this looks like "function creep" in the Data Protection area. The library community considers that data protection should apply to explicit personal data, but not the assumptions made in the report on behavioural data. We say this for two reasons: • Behavioural data is an important information resource to assist members in a library. • The other is that tracking outside the library needs to be considered an illegal activity. Until the technology is in place that prevents this (see the challenge libraries face in the previous comment) then this is an unnecessary burden on RFID operators like libraries.	
12.2.2	Table 10, Gap 2 Commentary (page 73)		**Proposed Comment:** The commentary only talks about the kill function invalidating multi-purpose use of tags. Libraries are far more concerned about multiple-re-use of the same tag for the same purpose. This needs to be addressed in the report as it is a more significant feature of many types of RFID application, not just libraries.	
12.2.2	Table 10, Gap 2.2 (page 73)		**Proposed Comment:** The library community already restricts the read range at self-checking stations, but has no control over the read range of the technology itself.	
12.2.2	Table 10, Gap 2.3 (page 73)		**Proposed Comment:** As indicated above, migration to a new tag technology will take years in a library environment. During this period, tags with different functional capabilities such as reduced read distance will need to be processed with old technology tags. In addition, the library community also needs to take into consideration the implications of this on the operation of the security gates.	
12.2.2	Table 10, Gap 3 (page 73)		**Proposed Comment:** While we accept the relevance of multi-purpose tags being included in this analysis, **we consider that a major omission is that nothing is stated about multiple re-usable tags.** This needs to be included, and it is obviously not our responsibility to provide text, but should be done by the report writers.	
12.3.1	Page 75, Air interface protocol Last bullet		**Proposed Comment:** The library community fully supports this analysis.	
12.3.1	Page 75, Air interface protocol Last para		**Proposed Comment:** Significantly reducing the read range might be acceptable in some circumstances, but will need serious consideration in the library community. It might well compromise the requirement to have security gates to guard against unauthorised removal of stock.	
12.3.1	Page 75, the interrogator		**Proposed Comment:** The library community would support the development of a standard that provided a mechanism so that all interrogators supporting 18000-3 Mode 1 had a means of unique identification that enabled unauthorised interrogators to be debarred.	
12.3.1	Page 75, Device Interface		**Proposed Comment:** The library community would welcome the development of a standardised API for authentication for interrogators that support ISO/IEC 18000-3 Mode 1 tags.	

12.3.1	Page 76, Data Encoding and Decoding		**Proposed Comment:** For those libraries that adopt ISO 28560, it is clear that no explicit personal data is encoded on the RFID tag on loan items. The inherent encoding rules for ISO 28560-2 provide a high level of data checking to protect against malicious data being intercepted by the library management system.	
Annex C.3	Page 85, 1st and 2nd para under fig C.1		**Proposed Comment:** The library community understands and supports specific PEN testing guidelines for RFID technology (tag and interrogator). However, it considers that a properly defined privacy impact assessment is sufficient to address the network connection to the back-end systems and the back-end systems themselves. Therefore, all the requirements set out in the second paragraph are considered to be an over-elaboration for standards, but essential in undertaking a privacy impact assessment. Standards for guidelines for penetration tests on the network communication and on the back-end system then only need to be based on a generic system. The second sentence of the second paragraph "We therefore need to identify and describe these RFID sectors and analyse their privacy and security needs." goes well beyond the need for sectors to take their own responsibility. It also appears to be in contradiction with a rigorous privacy and security assessment.	
Annex c.3	Page 85 last para continuing to top of page 86 – the 8 steps		**Proposed Comment:** This roadmap for RFID PEN testing standardisation needs to be considered on an "as-and-when" basis and would be better addressed generically on the technology rather than specifically by application as in steps 1, 2 and 3. The vulnerabilities are as much associated with the characteristics of the RFID tag and air interface protocol as for the specific applications. By focusing on the technology, it will provide the library community and other sectors with a strong foundation for the PIA. Going too deeply into the first stages of identifying applications will cause unnecessary delays and the work is best done through privacy impact assessment by people with expert knowledge of the applications. In other words, the focus of the penetration test should be built around the technologies that are being offered on the market and the PIA should be based on the specific application and the choice of those technologies.	
Annex C	Table C.1		**Proposed Comment:** We find terms such as "lack of respect" and "inappropriate/inadequate" an unnecessary slur on those who have developed and implemented RFID systems to date. It is unfortunate that the report was released with such terms, because we are aware that this was not the way these weaknesses were presented at the open meeting on 22 June 2010.	

Annex C	Table C.1 list of 20 vulnerabilities		**Proposed Comment:** This list of vulnerabilities seems to be haphazard. It would be better organised into at least the following four categories: • RFID technology • Data encoding • Data communication • Implications for the data subject/citizen By separating the vulnerabilities this way, it makes it far easier for a sector like the library community or even an individual library to understand where the vulnerabilities lie and to be able to address the threats properly. It also provides a significantly stronger demarcation of where the gaps in standards need to be addressed as opposed to implementation gaps.	
Annex D	Table pages 90 to 95		**Proposed Comment:** We note some significant misalignment in the labels (second of this table) and the labels in the objective column in Table 3 for many of the DPP objectives. This table needs to be correctly aligned with Table 3. It is not clear whether the text in the cells from the third column onwards refer to the DPPO-n or to the text in column two. This requires editing. We could not find any reference to DDPO-12 to 26 elsewhere in the report. Our specific comments (below) are focussed on the lettered and numbered text in the cells, so are unaffected by this editing error	
Annex D	Table page 90 Row DPPO-1, cell "A"		**Proposed Comment:** The library community's understanding is that a unique chip ID is required for access to the 18000-3 Mode 1 tags, and that the only standardised security that this tag offers is that of selective locking of blocks. So until a new tag technology is developed that meets the operational requirements of libraries and provides full interoperability with 18000-3 Mode 1 tags, the library community cannot see how additional security can be added at the tag and air interface level.	
Annex D	Table page 90 Row DPPO-1, cell "B"		**Proposed Comment:** We do not see the need for an explicit standard to deal with the control of data read by an application. As ISO/IEC 28560 is implemented, this – in itself – controls the set of data elements defined for the application.	
Annex D	Table page 90 Row DPPO-1, cell "C"		**Proposed Comment:** As indicated in previous comments, a feature that kills the tag is the exact opposite of the functionality required for the library community. Multiple Use Tags cannot support this function, so it is either not required, or needs to be switched off. Alternative options to reduce read range might be acceptable. Account needs to be given to the comments made above about the different data capture environments and reading distances for self-checkout and the security gates. Such a feature is not available in ISO/IEC 18000-3 Mode 1 tags, and the library community can only consider a tag with such a feature if its other characteristics meet the requirements for a library operation.	
Annex D	Table page 90 Row DPPO-1, cell "1"		**Proposed Comment:** The library community accepts the European Commission view that notification of an RFID-enabled implementation needs to be notified. It should also be noted, that every customer is aware of RFID through the self-checking transaction process.	

Annex D	Table page 90 Row DPPO-2, cell "2"		**Proposed Comment:** We do not see the need for an explicit standard to deal with informed consent. This should be part of the privacy impact assessment, with indications of where library customers need to provide informed consent.	
Annex D	Table page 90 Row DPPO-3, cell "D"		**Proposed Comment:** The table is proposing authentication across the air interface. From a technical perspective, we understand that this is difficult to achieve, particularly with the present generation of RFID tags. We are also concerned about the over-elaboration of the simple data communication requirements for reading and writing tags on loan items. Libraries would support authentication of membership cards at a reasonable cost. The cards are sometimes issued by a different authority than library management, so this issue is not always directly within the control of a library.	
Annex D	Table page 90 Row DPPO-3, cell "E"		**Proposed Comment:** It is not clear what "access control" means when applied to the reader. Therefore we cannot comment.	
Annex D	Table page 90 Row DPPO-4, cell "G"		**Proposed Comment:** We consider that by the introduction of ISO 28560 the library community has already addressed the issue of open system operational standards.	
Annex D	Table page 90 Row DPPO-4, cell "3"		**Proposed Comment:** Given the European Commission's interest in a privacy impact assessment, the library community accepts that such standards and procedures will be required. We feel that there is a requirement for some PIA guidelines around the technology. In the case of libraries, this is ISO/IEC 18000-3 Mode 1 for loan items, and the various card technologies. There should also be a generic PIA standard or guideline identifying the features that need to be considered. Thereafter, we consider that it is sector responsibility to prepare a PIA if this is possible. We consider that a generic PIA can be produced for the RFID application for libraries, which might address 80 to 90 % of an individual library's PIA. This would provide each library with information that is common across all, or many, libraries, and remove the burden from individual libraries of having to prepare the entire document unilaterally.	
Annex D	Table page 90 Row DPPO-5, cell "4"		**Proposed Comment:** The library community accepts the need for signage to indicate an RFID implementation. It opposes any requirement to apply an RFID logo to the individual loan items.	
Annex D	Table page 90 Row DPPO-7 & 8, cell "H"		**Proposed Comment:** The library community would support the development of an access control system between interrogators compliant with 18000-3 Mode 1, and the library management system. Due account needs to be taken of the fact that this RFID interface is currently proprietary and differs between manufacturers. Therefore, there is a requirement in developing this solution to take into account that it needs to be fairly easy to retro-fit in a variety of established implementations. We consider that reader authentication might probably be one of the better ways to move forward.	
Annex D	Table page 91 Row DPPO-9 to 11, cell "I"		**Proposed Comment:** The library community appreciates that a "privacy by design" process will probably result in some new technology standards. However, it is not clear how a privacy by design standard can be produced.	

Annex D	Table page 91 Row DPPO-13, cell "J"		**Proposed Comment:** We have some concern that any form of audit standard will be prescriptive. We consider that the PIA process, and associated registration is sufficient.	
Annex D	Table page 91 & 92 Row DPPO-14 to 16, cell "K"		**Proposed Comment:** As with the "privacy by design", we consider this to be more of a process. The mechanism to enable a person to access personal data (in the case of a library: from a card or on the library management system) can only be achieved by relevant (computer) procedures. It does not require an explicit standard. However, making a set of guidelines available might be helpful for some applications.	
Annex D	Table page 92 Row DPPO-17 to 19, cell "L"		**Proposed Comment:** We have some serious concerns about the three stated requirements in a multiple use application like a library. We accept that such features might be developed in a new generation of tags and relevant to other applications. These are our concerns: • **Tag deletion** is not acceptable in a library application, so such a feature cannot be automatic, and probably requires a switch to invoke it. • **Rendering Tag non readable (reversible)** might be possible, but account needs to be made that the security gate requirements are only applied after self checkout. Also the reversing process (a) needs to under the control of the library and (b) needs to be achievable at a low cost. • **Tag user selected non readability (reversible)** is not acceptable because it would make any loan item vulnerable to theft, or be used as a major denial of service threat to normal operations.	
Annex D	Table page 92 Row DPPO-17 to 19, cell "M"		**Proposed Comment:** Although the multiple application environment does not apply library loan systems, it does apply to some on the membership card used when the issuer is not the library management. There is no means at the RFID chip manufacturing stage of determining that the RFID tag / RF card will be used in a multiple application environment. Therefore there is no need for an explicit standard. Any development of new features for tag deletion, rendering a tag non readable (reversible), and making this user selectable needs to be assessed for single use, multiple use (as with libraries) and multiple applications.	
Annex D	Table page 92 Row DPPO-20, cell "N"		**Proposed Comment:** The library community considers that there are two steps to achieve this for ISO/IEC 18000-3 Mode 1 tags: • The system architecture standards for device interface, device management and data management need to be extended for operational purposes to support this tag. Given that there is a considerable installed base of this technology - not just in libraries – some other means of achieving this might need to be developed. • Then separately, or in parallel, privacy and security features need to be added	
Annex D	Table page 92 Row DPPO-20, cell "O"		**Proposed Comment:** We see system interoperability as a topic to be addressed by procedure, not standards.	
Annex D	Table page 92 Row DPPO-20, cell "5"		**Proposed Comment:** We see interoperability management as a topic to be addressed by procedure, not standards.	
Annex D	Table page 92 Row DPPO-22, cell "6"		**Proposed Comment:** As we are not sure what is meant, we have no comment. This point needs to be clarified.	

Annex D	Table page 93 Row DPPO-23, cell "P" and cell "7"		**Proposed Comment:** The library community considers that the penetration tests should focus on the air interface characteristics and vulnerabilities. Ideally there should be a procedural standard and a technical report identifying the results for each RFID technology in a manner that system designers can use. There is no need to extend this to the application, because this should be done during the step of the work should be done in the development of the PIA.	
Annex D	Table page 94 Row SO-5, cell "Q"		**Proposed Comment:** The penetration tests should be extended to address the security vulnerabilities of the tag, the air interface, the interrogator, and communication from the interrogator to the application. As stated above the results should be in a technical report identifying the results for each RFID technology in a manner that system designers can use. There is no need to extend this to the application, because this should be done during the step of the work should be done in the development of the PIA.	