SLOVENSKI STANDARD
SIST-TP CEN/TR 16674:2014

01-september-2014

Informacijska tehnologija - Analiza metodologij za ocenjevanje vpliva na zasebnost v povezavi z RFID

Information technology - Analysis of privacy impact assessment methodologies relevant to RFID

Informationstechnik - Analyse der RFID- Datenschutzfolgenabschätzung für spezifische Sektoren

Technologie de l'information - Analyse des méthodes d'évaluation de l'impact sur la vie privée adaptées à la RFID

Ta slovenski standard je istoveten z: **CEN/TR 16674:2014**

ICS:

35.040.50	Tehnike za samodejno razpoznavanje in zajem podatkov	Automatic identification and data capture techniques

SIST-TP CEN/TR 16674:2014 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16674

June 2014

ICS 35.240.60

English Version

Information technology - RFID privacy impact assessment analysis for specific sectors

Technologies de l'information - Analyse des méthodes d'évaluation de l'impact sur la vie privée adaptées à la RFID

Informationstechnik - Analyse der RFID-Datenschutzfolgenabschätzung für spezifische Sektoren

This Technical Report was approved by CEN on 20 January 2014. It has been drawn up by the Technical Committee CEN/TC 225.

CEN members are the national standards bodies of 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.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TR 16674:2014 E

Contents

Page

Foreword

This document (CEN/TR 16674:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC Technologies”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This Technical Report is one of a series of related deliverables, which comprise mandate 436 Phase 2. The other deliverables are:

— EN 16570, *Information technology — Notification of RFID — The information sign and additional information to be provided by operators of RFID application systems*

— EN 16571, *Information technology — RFID privacy impact assessment process*

— EN 16656, *Information technology - Radio frequency identification for item management - RFID Emblem (*ISO/IEC 29160:2012*, modified)*

— CEN/TR 16684, *Information technology — Notification of RFID — Additional information to be provided by operators*

— CEN/TS 16685, *Information technology — Notification of RFID — The information sign to be displayed in areas where RFID interrogators are deployed*

— CEN/TR 16669, *Information technology — Device interface to support* ISO/IEC 18000-3

— CEN/TR 16670, *Information technology — RFID threat and vulnerability analysis*

— CEN/TR 16671, *Information technology — Authorisation of mobile phones when used as RFID interrogators*

— CEN/TR 16672, *Information technology — Privacy capability features of current RFID technologies*

— CEN/TR 16673, *Information technology — RFID privacy impact assessment analysis for specific sectors*

Introduction

In response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM (2007) 96 'RFID in Europe: steps towards a policy framework'. This Communication proposed steps which needed to be taken to reduce barriers to adoption of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

In December 2008, the European Commission addressed Mandate M/436 to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems. The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information aspects of RFID, and is being executed in two phases. Phase 1, completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report TR 187 020, which was published in May 2011.

Phase 2 is concerned with the execution of the standardization work program identified in the first phase.

This Technical Report is one of eleven deliverables for M/436 Phase 2. From a content point of view, and despite their name, most Privacy Impact Assessments in the world have a narrow focus, namely data protection rather than privacy protection. The result is that many PIAs are restricted to legal compliance checks and do not include societal aspects. That is reflected in the form of some PIAs, which are limited to checklists. Increasingly, however, PIA methodologies include narrative descriptions of the systems assessed and the environments in which they will operate, which help to understand better the potential privacy and data protection risks.

Also most PIAs are limited to risk assessment and do not include risk management. Thus, they can be used to identify and assess privacy and data protection risk without suggesting solutions or mitigation strategies, thereby restricting their usability.

This deliverable will begin with research of methodologies used for wireless technologies and the risks associated at within that part of the wireless system from the data carrier to the communication from the 'interrogator' or data capture device to the application system. The reason for this approach is to understand approaches used by security experts and that are not incorporated into any existing standards. This approach makes sense because it moves from the generic wireless towards the specific RFID issues. The intention is to draw relevant 'lessons' from a range of wireless technologies that can be applied to RFID technologies and applications. Risk management will focus on areas that accept the inherent risks of the given technology.

1 Scope

The scope of this Technical Report (TR) is to identify methodologies that are used for, or have been considered applicable to, wireless technologies. These methodologies are analyzed to identify features that are applicable to RFID.

Based on the Industry RFID PIA Framework endorsed by the Article 29 Data Protection Working Party, the Technical Report focuses on proposing risk analysis methodologies suitable for the data capture area of an RFID system. This includes the RFID tag, the interrogator, the air interface protocol used for communication between them, and the communication from the interrogator to the application.

The Technical Report also proposes risk management features based on the inherent capabilities of a number of RFID technologies that conform to standardized RFID air interface protocols. This should provide enough information to enable the proposed privacy control features to be applied to other RFID technologies including those with proprietary air interface protocols and tag architectures. The risk management features exclude fundamental privacy by design features because these should be the subject of revisions and enhancements to technology standards. The risk management features defined in this Technical Report are considered applicable to current and future implementations of RFID based on existing technology. As such, this Technical Report is considered as input into a standard procedure for undertaking an RFID Privacy Impact Assessment.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
controller
natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

2.2
data subject
identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

2.3
data subject's consent
any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

2.4
personal data
any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

2.5
PIA process
process based on a privacy and data protection risk management approach focusing mainly on the implementation of the EU RFID Recommendation and consistent with the EU legal framework and best practices

2.6

privacy
the claim of individuals (...) to determine for themselves when, how and to what extent information about them is communicated to others" and as a mean "(...) for achieving individual goals of self-realisation

2.7
privacy impact assessment
methodology (a systematic process) for assessing the impacts on privacy of a project, policy, program, service, product or other initiative that involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative privacy impacts

2.8
processing
any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as reading, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction

2.9
processor
natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

2.10
accountability
responsibility of an organization for personal information in its possession or custody, including information that has been transferred to a third party for processing

2.11
wireless network
any type of computer network that is not connected by cables of any kind

3 Symbols and abbreviations

CEN Comité Européen de Normalisation

COBIT Control Objectives for Information and related Technology

DPD Directive Personal Data

NOTE 1 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

DPIA Data Protection Impact Assessment

DPR General Data Protection

NOTE 2 Regulation on the Protection of Individuals with regard to the processing of personal data and on the free movement of Such Data

ECHR European Convention on Human Rights EU: European Union

ECtHR European Court of on Human Rights

ENISA European Network and Information Security Agency

GDPR General Data Protection Regulation

ITIL Information Technology Infrastructure Library

NFC Near Field Communication

NIST National Institute of Standards and Technology

OECD Organization for Economic Co-operation and Development

PBD Privacy by Design

NOTE 3 Related to Data Protection.

PCC Privacy Commissioner of Canada

PIA Privacy Impact Assessment

PLD Personal Locating Device

RTLS Real Time Location Systems

SDLC System Development Life Cycle

TAS3 Trusted Architecture for Securely Shared Services

NOTE 4 EU research project Trusted Architecture for Securely Shared Services, Privacy Requirements, v.2.0, 2009

TDOA Time Difference Of Arrival

TRA Threat and Risk Assessment

Tri Triangulation

WAP Wireless Access Point

WiFi Wireless Ethernet

4 Risk analysis for wireless RFID communications and RFID devices

4.1 Introduction

As stated in the scope, the TR is to identify methodologies that are used for, or have been considered applicable to, wireless technologies. These methodologies are analyzed to identify features that are applicable to RFID. Furthermore, based on the Industry RFID PIA Framework endorsed by the Article 29 Data Protection Working Party, the TR focuses on proposing risk analysis methodologies suitable for the data capture area of an RFID system. This includes the RFID tag, the interrogator, the air interface protocol used for communication between them, and the communication from the interrogator to the application.

The RFID PIA framework is based on Opinion 9/2011 on “The Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications”. Opinion 9/2011 has been influenced by the requirements mentioned in the analysis of ENISA Position on the *Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010]* July 2010

The title of Recommendation (2009/387/EC) makes it very clear that the Commission has an objective to see the implementation of privacy and data protection principles in RFID applications, and for this to be partly achieved by RFID operators undertaking a privacy impact assessment (PIA). Much of the work approved under Mandate M436 Phase 2 extends this principle into more practical processes.

Unfortunately there is no evidence of a standards-based procedure for undertaking a PIA for applications using RFID technology. The TR therefore focuses on three strands of research:

— principles that are appropriate to RFID based on the research undertaken to prepare this TR;

— analysis of PIAs that are relevant to the RFID PIA, but not directly associated with RFID, from five countries (Australia, Canada, New Zealand, UK and USA) and discussed more fully in Clause 7;

— comparison between the intended approach and some European interim developments.

4.2 RFID technologies

The Recommendation, provides the following definition of RFID in Paragraph 3 (a):

'Radio frequency identification (RFID)' means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag

This means that RFID applies to all RFID technologies specified by the ISO/IEC 18000 series of standards plus what some experts consider to be a different technology: smart cards. Thus, ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 18092, ISO/IEC 21481, and the Japanese FeliCa (JIS X6319-4) all fall within the scope of the Recommendation. In fact any standardized or proprietary radio frequency technology operating within the regulated ranges, as listed here, fall within the scope of the Recommendation:

— <125 kHz to 134 kHz

— 13,56 MHz

— 433 MHz

— 860 MHz to 960 MHz

— 2,45 GHz

— 5,8 GHz (although there are no standards in the ISO/IEC 18000 series that address this yet.

NOTE Further details of the RFID privacy capabilities are provided in CEN/TR 16672 Information technology - Privacy capability features of current RFID technologies.

4.3 The RFID system architecture

Each RFID air interface protocol has different characteristics; the most obvious is the frequency at which the protocol operates. This impacts on power capabilities and read range. Even at a given frequency there are often multiple protocols, each of which offers the RFID application particular features. Currently the ability to have interoperable protocols is low. Interoperability between frequencies is rare, because the laws of physics vary according to frequency particularly between low frequency (125kHz to 133 kHz) and high frequency (13,56 MHz) on one hand and all the other higher frequencies.

Each specific air interface protocol defines the communication rules between the RFID interrogator (or reader) and the RFID tag. There are no explicit standards for the interrogator and the tag; instead products are required to conform to mandatory components of the protocol, and may support some of the optional features. Such optional features include the size of memory, even whether some defined areas of memory are supported. The optional features also include a number of commands, e.g. the support for sensors but also more basic features. For a given air interface protocol, tags have more optional (i.e. opt-out) features than interrogators; but this does not mean that interrogators are required to support all the features of a protocol. Generally an RFID application is built around a particular air interface protocol, and there can be many variants in the capabilities of tags that are available. In true open systems the RFID operator is dependent on the RFID tags (and hence their capabilities) provided by others in the value chain. Although not a truism, a rule of thumb is that tags with increasing capabilities tend to be more expensive; so the purchaser of the tags will tend not to over-specify requirements for capabilities. Until the Recommendation was published, few RFID operators consider privacy requirements, and CEN/TR 16672 clearly identifies that potential privacy enhancing features are not available in many RFID technologies.

Some of the protocols are considered fairly stable with little or no developments over recent years. Others, particularly ISO/IEC 18000-63, are under continual development with more features added with each revision. This adds to the complexity, because whereas tags with new features can be implemented reasonably quickly, changing the interrogator infrastructure involves longer-term investment decisions. But even if some advanced tags are introduced, not all tags in an application will change. This is particularly the case where the RFID tag or smart card has a viable life of many years.

The air interface is based on wireless communications, and as such is vulnerable to noise, which interferes with the communication, and to various threats. Because the interface is wireless, most protocols have no

means of restricting additional reads of the tag. In fact, in open systems it is essential that the tag remains readable to any authorised reader. Conversely this can also be exploited, as indicated by CEN/TR 16672. Additionally other mechanisms can be used to read data, such as eavesdropping. As RFID is a read / write technology, it is also possible to change data on the tag again for legitimate reasons (e.g. a chain of custody) and less legitimate reasons.

Besides the tag, the air interface protocol and the interrogator, there are other components to the RFID system. The interrogator needs to communicate with the application to receive instructions that are converted to air interface commands, and to send back responses from the tag e.g. the data read form the tag. The air interface transmits bits of data that need to be created (commands) and interpreted (responses). Device interface protocols and data encoding and decoding rules are needed to perform some of these functions. Not all air interface protocols and applications use standardized rules for this, although this is increasing – and essential in open system applications. Some specific standards are discussed in CEN/TR 16673: *Information technology - RFID privacy impact assessment analysis for specific sectors.*

In some cases the communication between interrogator and application is carried out over wired networks, but this requires readers to be in fixed locations. Wireless communications are also, and increasingly used, particularly with RFID enabled smart-phones and tablet computers. A particular case is with the use of near field communication (NFC). This can bring additional opportunities to the individual smart-phone owner. Where these are designed applications authorised by the RFID operator, this enhanced functionality adds to the application. But the other side of the coin is that making millions of smart-phones as RFID readers does have potential negative implications discussed below.

4.4 The challenge of having millions of readers in the hands of individuals

It is fairly easy to create an RFID reader, by using in-built features of NFC-enabled smart-phones. Originally focused on one air interface protocol dealing with smart cards, there are concerns that there is technology creep and these phones are able to read (and write) to tags compliant with other HF protocols. Some RFID operators are extending their applications to make use of the fact that RFID readers are increasingly present. The positives are addressed, but less so the negative aspects. These fall into two broad categories:

— The capability to change data on the tag, which can lead to disruptions of the intended application e.g. even to render the tag unreadable. This is predominantly a security issue for the application, but does have privacy implications too.

— The capability to read data from the tag beyond the scope of the application and beyond the domain of the RFID operator.

There have been developments for smart-phones to support the UHF-based protocols, particularly from Korea, but development has been slower than expected. However, it is feasible. Furthermore, there are many readers for most of the popular readers that can be connected to a USB port, some looking little different than a memory stick.

All of this means that individuals holding RFID tags or smart cards are probably unaware that tags and cards that they are holding can be read beyond the boundary of a particular RFID application. Some evidence has been presented in CEN/TR 16673; one example is of the recent capability to change data on RFID tags in the library sector, another is the capability to read data from some contactless payment cards.

Thus, intruders can launch denial of service attacks, steal identities, violate the privacy of legitimate users, insert viruses or malicious code, and disable operations.

The draft version of CEN/TR 16674: *Information technology - RFID privacy impact assessment analysis for specific sectors* identifies a number of threats that have been recorded in literature and shown to be possible. As a protocol reaches a critical mass of tags or cards in circulation, combined with low cost reading devices capable of reading the tags, this type of issue will spread. A properly structured PIA process can identify the risks and countermeasures that might be implemented.

4.5 Lessons from the risk environment concerning wireless networks

All computer systems are subject to different forms of threat, but wireless networks can suffer from additional threats because of the fact that there are various means of intercepting a wireless transmission that are not possible with a wired network. For RFID this applies to the air interface and wireless communication between the interrogator and the application. The US-based National Institute of Standards and Technology (NIST) recommends that before establishing wireless networks and using handheld devices, organizations should use risk management processes to assess the risks involved, to take steps to reduce the risks to an acceptable level, and to maintain that acceptable level of risk. Using risk management processes, managers can protect systems and information in a cost-effective manner by balancing the operational and economic costs of needed protective measures with the gains in mission capability to be achieved through the application of new technology.

The following is an abstract from NIST's report "Security for Wireless Networks and Devices". Apart from some details, this information is considered highly relevant to RFID.

NIST points out that each new development will present new security risks, which shall be addressed to ensure that critical assets remain protected. Actions that organizations should take to protect the confidentiality, integrity, and availability of all systems and information include:

a) Assess risks, test and evaluate system security controls for wireless networks more frequently than for other networks and systems. Maintaining secure wireless networks is an ongoing process that requires greater effort than that required for other networks and systems.

   The following steps that can be taken to improve the management of wireless networks include:

   — Maintain a full understanding of the topology of the wireless network.

   — Label and keep inventories of the fielded wireless and handheld devices.

   — Create backups of data frequently.

   — Perform periodic security testing and assessment of the wireless network.

   — Perform ongoing, randomly timed security audits to monitor and track wireless and handheld devices.

   — Apply patches and security enhancements.

   — Monitor the wireless industry for changes to standards that enhance security features and for the release of new products.

   — Monitor wireless technology for new threats and vulnerabilities.

b) Perform a risk assessment; develop a security policy and determine security requirements before purchasing wireless technologies.

   The risks associated with the use of wireless technologies are considerable, and many products provide inadequate protection. Organizations should plan to protect their essential operations before they adopt wireless technologies. Common administration problems include installing equipment with "factory default" settings, failing to control or inventory access points, not implementing the security capabilities provided, and not developing or installing security architectures that are suitable to the wireless environment. The use of firewalls between wired and wireless systems should be considered. Other good practices are to block unneeded services and ports, and to use strong cryptography. Often the risks can be addressed, but the tradeoffs between technical solutions and costs shall be considered as well. Organizations may want to postpone the installation of wireless networks until more robust, open, and secure products are available.

Organizations should perform security assessments prior to implementation of wireless technologies to determine the specific threats and vulnerabilities that wireless networks will introduce in their environments. In performing the assessment, they should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs of security measures, and technical requirements. Once the risk assessment is complete, the organization can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The organization should periodically reassess the policies and measures that it puts in place because computer technologies and malicious threats are continually changing.

c) Effective risk management should be integrated into the System Development Life Cycle (SDLC) of an IT system. The SDLC includes five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. NIST has issued recommendations for conducting the risk management process in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. This document is available online at http://csrc.nist.gov/publications/nistpubs/index.html.

d) Maintain an awareness of the technical and security implications of wireless and handheld device technologies.

Wireless technologies present unique security challenges due in part to the relative immaturity of the technology, incomplete security standards, flawed implementations, limited user awareness, and lax security and administrative practices. In a wireless environment, data is broadcast using radio frequencies. As a result, data may be captured when it is broadcast. The distances needed to prevent eavesdropping vary considerably because of differences in building construction, wireless frequencies and attenuation, and the capabilities of high-gain antennas. The safe distance can vary up to kilometers, even when the nominal or claimed operating range of the wireless device is less than a hundred meters.

e) Carefully plan for the installation of wireless technologies.

The security of wireless networks and devices should be considered from the initial planning stage because it is much more difficult to address security once deployment and implementation have occurred. A detailed, well-designed plan can point the way to better security decisions about configuring wireless devices and network infrastructure. The plan will support decisions concerning the tradeoffs between usability, performance, and risk. It is necessary to apply security management practices and controls to maintain and operate secure wireless networks.

f) Organizations should identify their information system assets, and develop, document and implement policies, standards, procedures, and guidelines to ensure confidentiality, integrity, and availability of information system resources. NIST recommends the following steps:

— The information system security policy should directly address the use of 802.11, Bluetooth, and other wireless technologies.

— Configuration/change control and management practices should ensure that all equipment has the latest software release, including security feature enhancements and patches for discovered vulnerabilities.

— Standardized configurations should be employed to reflect the security policy, and to ensure change of default values and consistency of operations.

— Security training is essential to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies.

— Robust cryptography is essential to protect data transmitted over the radio channel, and theft of equipment is a major concern.

g) Physical controls should be implemented to protect wireless systems and information.

Adequate physical security measures include barriers, access control systems, and guards. Physical countermeasures can lessen risks such as theft of equipment and insertion of rogue access points or wireless network monitoring devices. The small size, relatively low cost, and constant mobility of handheld devices make them more likely to be stolen, misplaced, or lost, and the physical security controls that protect desktop computers do not offer the same protection for handheld devices.

h) NIST recommends to enable, to use and routinely to test the inherent security features, such as authentication and encryption methods that are available in wireless technologies. Firewalls and other appropriate protection mechanisms should also be employed.

Wireless technologies generally come with some embedded security features, although frequently many of the features are disabled by default. The security features available in wireless networks and devices may not be as comprehensive or robust as necessary. The security features provided in some wireless products may be weak; therefore, robust, well-developed, and properly implemented cryptography should be used to attain the highest levels of integrity, authentication, and confidentiality.

The built-in security features of Bluetooth and 802.11 networks can include data link level encryption and authentication protocols, and these features should be used as part of an overall defense-in-depth strategy. Although these protection mechanisms may have weaknesses, they can provide a degree of protection against unauthorised disclosure, unauthorised network access, and other active probing attacks.

The data link level wireless protocol protects only the wireless sub-network. Where traffic traverses other network segments, including wired segments or the organization's backbone network, other end-to-end cryptographic protection may be required. Since there is still a residual risk when cryptography and other security countermeasures are used, it may also be necessary to provide strategically located access points, firewall filtering, and antivirus software.

4.6 Conclusion and a way forward

The recommendations of NIST can be used *mutatis mutandis* for the RFID applications. It should be noted that NIST recommendations are for wireless networks and hence applicable when an application read operation is undertaken within the application domain. However RFID identifiable items in the possession of individuals pass beyond the application boundary and are potentially subject to conditions and attacks that are outside the control of the main network and so the protective capability of the RFID tag is the main focus for assessment for such situations.

The approach calls for a formal risk assessment procedure taking into account threats and vulnerabilities. There are no international standards that address RFID and its associated privacy risk assessment. However, ISO/IEC 27005 provides some methodologies for carrying out risk assessments and these have also been adopted and adapted by ENISA, but not explicitly for RFID.

Three metrics are required:

— A valuation of assets in the application. For RFID and privacy this needs to be based on the "value" of explicit personal data or identifiable data encoded on the RFID tag. This would include unique chip identifiers that are present in most RFID technologies. ISO/IEC 27005 score assets in a range from 0 (no value) to 4. Given the early stages of developing an RFID PIA this level of granularity seems reasonable.

— Threats associated with the technology need to be considered. There is sufficient literature on RFID threats for these to be identified and taken into consideration. In ISO/IEC 27005 threats are defined as low, medium or high.

— Vulnerabilities identify the opportunities to exploit a threat. Again ISO/IEC 27005 has a simple metric of low, medium and high.