EN 16571 RFID Privacy Impact Assessment CNRFID- CSL Software

Do you know that there are European Standards that define rules for undertaking an RFID privacy impact assessment (PIA), and for notifying users that RFID data capture is taking place?

Are you aware that the new European General Data Protection Regulation (GDPR) calls for privacy impact assessments to be undertaken?

The European Standard **EN 16571:2014, *Information technology – RFID privacy impact assessment process***, has been published by all 33 European national standards bodies. The standard defines a process that should be implemented by organisations that operate RFID applications in Europe. The European Commission has made it clear that the scope of the RFID PIA covers all radio frequency technologies, including smart cards and contactless payment using RF frequencies.

The core to the process is a **privacy risk assessment** based on the particular RFID technology being used in an application. The quantified risk assessment comprises:

1) identifying and assigning values to data on the RFID tag and application associated with an individual's privacy;
2) identifying technology related threats to the RFID system and providing a means of assessing the threat level;
3) identifying vulnerabilities and enumerating the associated risk levels;
4) arriving at an initial risk level, before considering any countermeasures;
5) considering the technology related countermeasures that can be used to reduce the threat level, which results in the residual risks associated with each asset in the RFID application.

A joint effort by the French National RFID Centre (CNRFID) and Convergent software Ltd (CSL) has resulted in fully compliant software that supports the most commonly used protocols but will eventually cover all RFID technologies. EN 16571 uses a method adapted from ISO/IEC 27005 for determining a risk value based on values assigned to assets, threats and vulnerabilities. The software enables a semi-automated RFID privacy impact assessment to be produced based on the data on the tag, the specific RFID technology being used, even down to the product level. The net result is a fully compliant PIA of the specific RFID system. How can this work? Let's consider the five points above in more detail.

1 Assigning asset values to data

EN 16571 defines a list of types of data that can be encoded on the RFID tag and on the host application. EN 16571 assigns a value 0 to 4 to a data type. Using the software, the person or team developing the PIA, select the relevant data types. These have pre-assigned values, which can be modified. The highest value data type is assigned to the privacy asset, e.g. the RFID tag, membership card, or smart card being use in the application.

2 Identifying technology related threats

CNRFID-CSL maintains a database of RFID products and their privacy related features. When the software is installed, product choices are already focused on the protocol being used. Therefore only threats that are relevant to the specific RFID protocol are presented. All the threats, such as unauthorised tag reading or a Man-in-the-Middle attack are identified and have a risk score. EN 16571 assigns a value 0 to 2 to a threat.

3 Vulnerabilities and risk levels

Unlike software and network vulnerabilities, there is no established procedure or organisation like United States Computer Emergency Readiness Team (US-CERT)[1] to identify vulnerabilities and assess their risk factors. EN 16571 has taken a basic but pragmatic approach to an RFID vulnerability. If it is impossible to implement a threat, then the vulnerability risk level is defined as 'low' and given a score of 0. If a threat is identified as feasible to apply to the RFID technology used in the application, then its vulnerability risk level is 'medium' to indicate that the threat and implied vulnerabilities have been identified and tested in research documents. The vulnerability level of 'high' only applies when known exploits have been identified in real applications. **Unfortunately there are some.**

4 Arriving at an initial risk level

The risk scoring method is on defined in ISO/IEC 27005 and shown in the table below:

	Likelihood of Threat	Low			Medium			High		
	Ease of Exploitation - Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

All the calculations are carried out automatically by the CNRFID-CSL software.

5 Technology-related countermeasures and risk reduction

Countermeasures are the means to reduce the privacy risk of holding an RFID tag or smart card. Any single countermeasure can address more than one threat and a given threat can have its risk reduced by more than one countermeasure. EN 16571 identified 49 countermeasures and proposes a simple rule for the impact of a countermeasure. If any countermeasure is applied, then the risk level is reduced by 1.

The CNRFID-CSL is significantly more sophisticated in these ways:

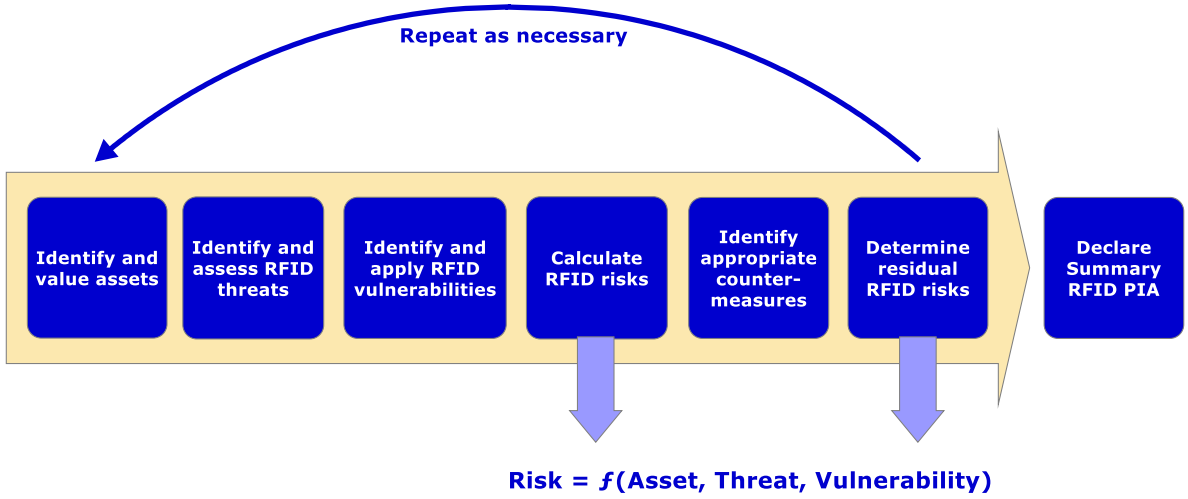
- Because of the expanding database of products, countermeasures that are supported by the tag and reading device are identified in addition to the basic protocol level countermeasures.
- Some RFID product manufacturers have shown increasing responsibility about privacy and introduced additional countermeasures on new products, such as being able to reduce read range after the tag has been read.
- New privacy enhancing features added as countermeasures in the CNRFID-CSL software as they are identified, making the software more dynamic than the standard.

[1] https://www.us-cert.gov/

- The software has an inbuilt ***smart algorithm*** that enables multiple countermeasures to be processed against multiple threats. This shows the resultant risk reduction of all the countermeasures producing a **residual risk** value of the RFID system.

The CNRFID-CSL software delivers details of all the countermeasures as they apply to each RFID asset being used in the RFID system. For example, in a hospital there could be a tag on medical records, the hospital bed and equipment, medical staff Id badges, support staff id badges (e.g. cleaning contractors), and even the patient.

This fact that some countermeasures are available but not implemented enables those controlling the RFID system to consider carrying out a 'what if' procedure and re-run the PIA process with additional countermeasures as illustrated here:



The software contributes to a **privacy-by-design** process by providing a facility to write an improvement plan, which should consider:

- technology based countermeasures that have not been applied
- modifying the business processes
- upgrading tags and possibly interrogators
- even providing users with the means to protect the RFID tags or cards they hold

It is not possible to implement every technical countermeasure, even those supported by the RFID tag and reader being used. Such changes might require operational aspects of the system to change, for example, with a software upgrade.

But, as with all privacy and data protection issues, the threat landscape can change and the vulnerability increases because of other developments or deliberate malpractice. Some years ago RFID devices were considered 'business only' and sold B2B. For some protocols there are now over three quarters of a billion reading devices in the hands of members of the public. These devices are called smart phones. Also as the popularity of RFID increases and more systems are implemented, hackers and others will target such applications. Already there are devices being marketed on the dark web that threaten RFID privacy and even system security.

The first step is implementing a robust and consistent RFID privacy impact assessment to establish the initial risk and identify countermeasures that can be applied. Then progressively further improvements can be made to achieve privacy-by-design.

Because of the CNRFID-CSL software has been developed by a team with deep knowledge of RFID technology standard, protocols. As such CNRFID-CSL can keep abreast of new developments in threats and countermeasures. The RFID PIA software will be continually and automatically updated.