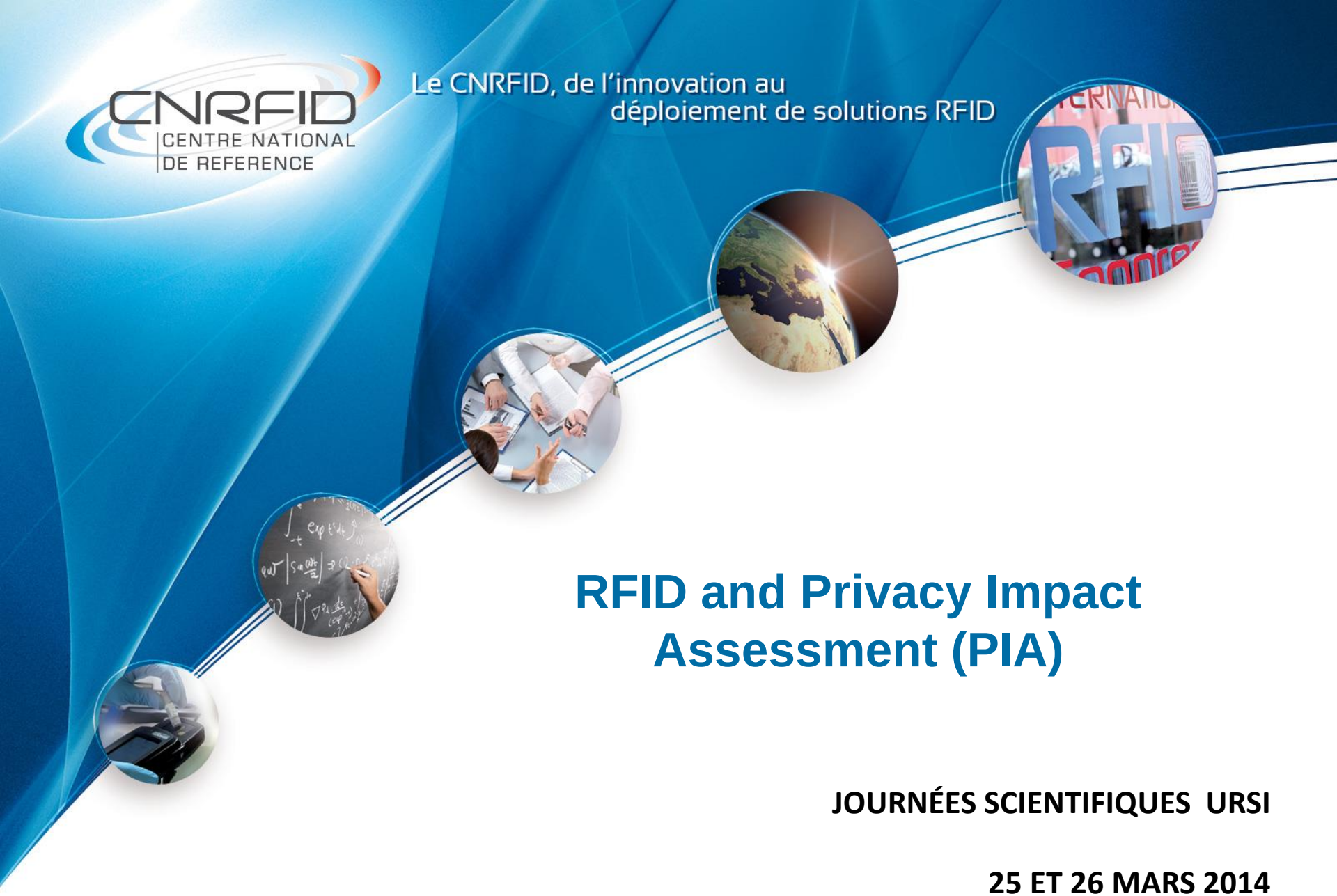
CNRFID
CENTRE NATIONAL
DE REFERENCE

Le CNRFID, de l'innovation au
déploiement de solutions RFID



RFID and Privacy Impact Assessment (PIA)

JOURNÉES SCIENTIFIQUES URSI

25 ET 26 MARS 2014

Agenda

- ✓ Introduction: RFID everywhere?
- ✓ RFID and security issues
- ✓ RFID threats
- ✓ The European Recommendation
- ✓ Privacy Impact Assessment Process
- ✓ Signage and public awareness
- ✓ Conclusion

RFID everywhere?

- ✓ **Citizen use more and more RFID technologies**
  - **Ticketing (transportation and events)**
  - **Payment (small values w/o PIN code)**
  - **Identity (passport, driver licence)**
  - **NFC applications…**
- ✓ **Citizen are surrounded by RFID tags**
  - **Everyday life products (textile, library books,…)**
  - **Luxury goods (authentication, certificates,…)**
  - **First developed for logistics, inventory, article surveillance, …**
- ✓ **Data can be identify people directly…**
  - **Name, address, etc.**
  - **Generally secured HF protocols (first use cases)**
- ✓ **Or indirectly**
  - **Unique identifiers (TID, EPC, …)**
  - **Combined with other data, could impact privacy**

Security issues

- ✓ **RFID for item identification is a weak technology (up to now…)**
  - ➢ Low cost, limited resources, finite-state machine
  - ➢ Does not support cryptography (except proprietary products)
  - ➢ No mutual authentication
- ✓ **Most of RFID chips have a Unique Identifier (TID)**
  - ➢ TID can be serialized
  - ➢ TID is programmed once by the chip manufacturer
  - ➢ Cloning is possible but requires special skills
- ✓ **Data can be stored in the tag memory or in a external secured database**
  - ➢ GS1 EPCIS : Information can be accessed via EPC after internet authentication
  - ➢ For many applications (aircraft maintenance, health, open loop applications,…) some data have to be stored in the tag memory
- ✓ **New standards propose security features**
  - ➢ 29167-1 : Air interface for security services and file management for RFID architecture (SC31/WG7)
  - ➢ 29167-1x: Crypto suites (UHF et HF)
  - ➢ EPC Gen2V2 proposes commands to support ISO crypto suites

RFID Threats

- ✓ **RFID Threats are mainly based on two different attacks:**
  - **Eavesdropping**
  - **Tag activation**

- ✓ **Eavesdropping**
  - **Listening the communication between a tag and an interrogator**
  - **Eavesdropping distances are greater than reading distances**
  - **Information can be decoded if not cover-coded or encrypted**

- ✓ **Tag Activation**
  - **RFID tag are operational once energized (no ON/OFF switch)**
  - **A fake reader can ask a real tag to backscatter information**
  - **Activation distances are greater than reading distances because attacker does not care Regulation limitations (eg. 2Werp in Europe)**

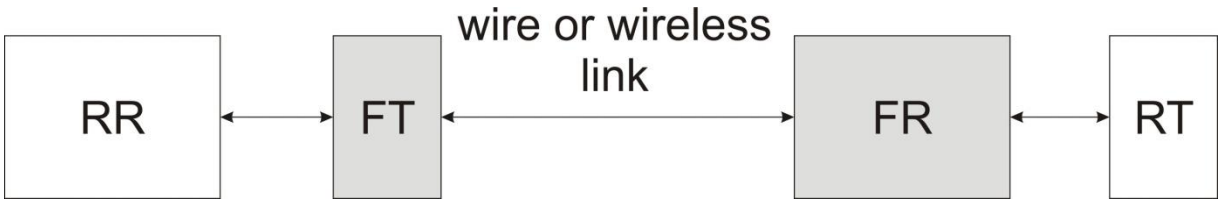
- ✓ **Actual threats are a mix of eavesdropping and tag activation**

Examples of RFID Threats

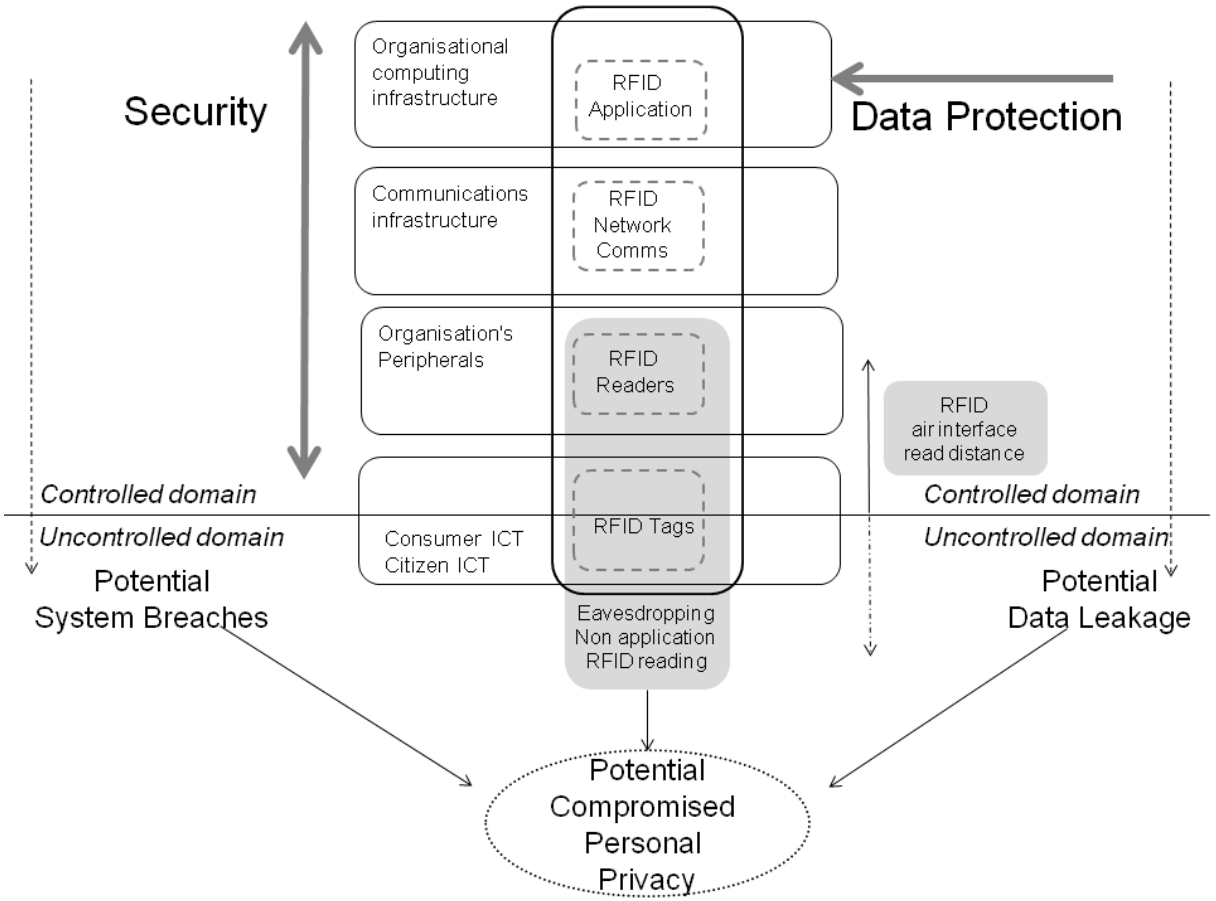
- ✓ **Physical data modification:**
  - ➢ **unauthorized changing of encoded data on the tag by deleting, modifying or adding data**
  - ➢ **Example: changing a product code to gain some financial advantage**

- ✓ **Tracking**
  - ➢ **Continual sequence of unauthorized tag reading**
  - ➢ **The threat can be deployed with mobile or fixed interrogators**
  - ➢ **Example: tracking of employees in known zones, tracking of customers,…**

- ✓ **Relay Attack**
  - ➢ **Also known as "Man in the middle" attack**
  - ➢ **Allow a real tag to communicate with a real reader at long distances**
  - ➢ **Example: Access a building without authorization**



Privacy, Security, data protection



privacy is the individual's right to determine the use of any information about him

Privacy

Main legal reference texts :

US : Privacy Act (1974)

France : Loi informatique et libertés (1978) modifiée le 6 août 2004

EU : Convention n°108 of European Council (1981) : reconcile respect for privacy and free flow of information

EU : Directive 95/46/CE : protection of individuals with regard to the processing of personal data and on the free movement of such data

EU : Chart of fundamental rights of the UE (2000) (Art. 8, right to the protection of personnal data)

EU : Directive 2002/58/EC : (directive e-privacy) translate principles of directive 95/46/CE in specific rules for Telecommunication sector

EU : Recommandation May 2009 (RFID)

EU : EN 16571 to be published in 2014 (RFID Privacy Impact Assessment)

Privacy (European Recommendation)

Due to potential massive RFID deployment, the European Commission issued a Recommendation (May 2009)

« on the implementation of privacy and data protection principles in applications supported by RFID »

✓ Title

- **« Data protection » : <u>not only</u> personal data protection**

✓ Definitions & Scope

- **All RFID technologies (NFC and contactless smart cards included)**
- **All kind of application, except… governmental applications**
- **Focus on retail sector (direct link to the consumer)**

Privacy (European Recommendation)

- ✓ **Focus on tag deactivation at the Point of Sale**
- ✓ **Logic**
  - ➢ **Secured deactivation (Kill + passwords)**
  - ➢ **Unsecured deactivation (Kill)**
- ✓ **Hardware**
  - ➢ **Tag destruction (strong electromagnetic wave,…)**
  - ➢ **Tag removal**

Privacy (Recommandation)

- ✓ **Recommendation does not oblige to deactivate the tags at PoS if RFID operator undertakes a Privacy Impact Assessment (PIA) and proves that the risk is limited**
  - ➢ **Systematic deactivation (OPT-IN) in case of high level of risk.**
  - ➢ **To provide a simple, immediate and free way to disable the tag at PoS (medium level of risk) (OPT-OUT)**

- ✓ **Privacy Impact Assessment (PIA)**
  - ➢ **Identify the impact of the implementation of the application with respect to personal data and privacy**
  - ➢ **PIA has to be undertaken by the RFID operator**
  - ➢ **Level of detail consistent with risk level**

Examples

- ✓ Payment card
  - ✓ contains personal information => level 3
- ✓ Management of library books
  - ✓ data in the tag are linked to personal information, but these personal information are not in the tag memory => level 2
- ✓ Packaging consumables
  - ✓ RFID tags are used for logistics
  - ✓ Packaging are discarded / recycled by the consumer
  - ✓ an individual may have an RFID tag of this application at a given time => level 1
- ✓ Industrial maintenance
  - ✓ monitoring train axles, …
  - ✓ no personal data in the application, unlikely that an individual is in possession of this type of tag => level 0

Risk value (EN 16571 / ISO 27005)

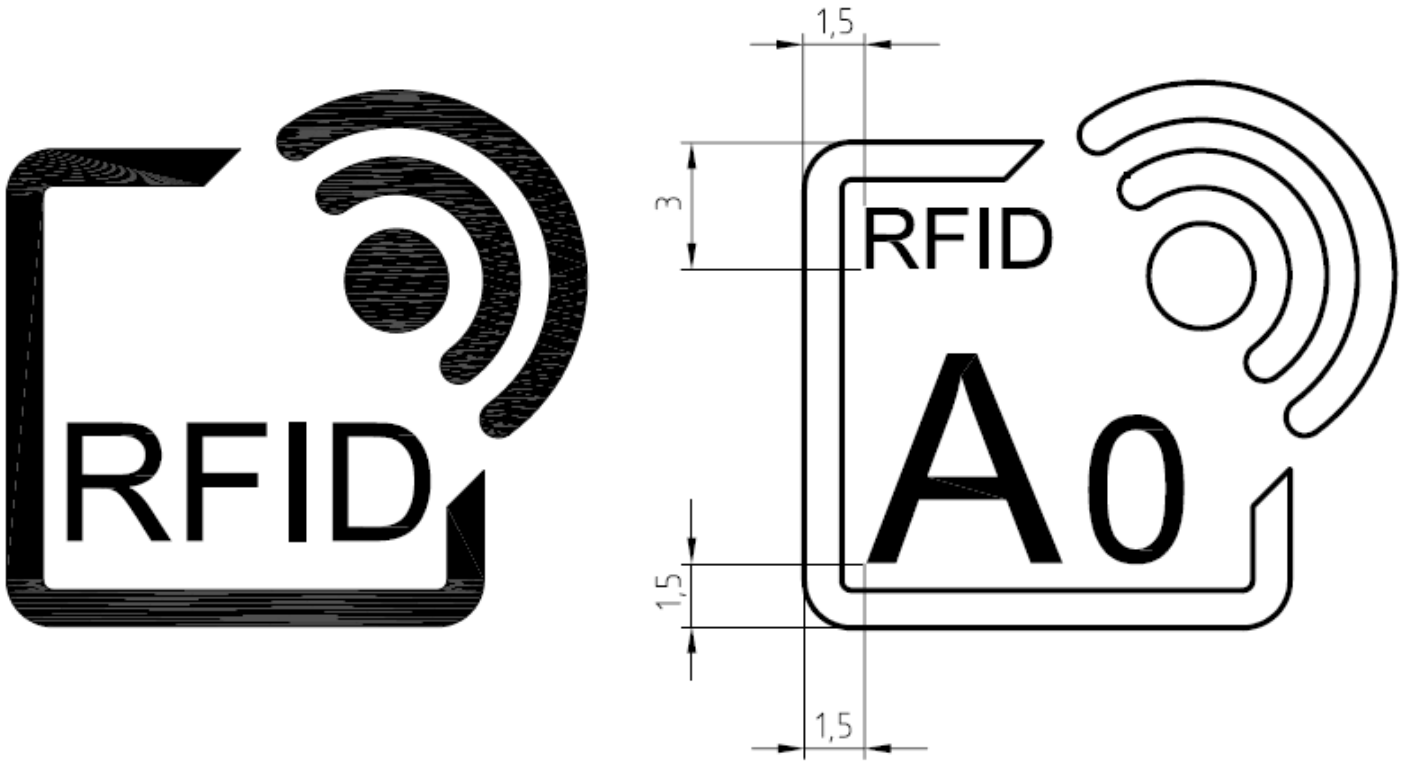
	Likelihood of Threat	Low			Medium			High		
	Ease of Exploitation - Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

- ✓ **Example: library book**
  - **Asset Value 2 (Unique Identifier linked to book category)**
  - **Threat Medium (Tag activation)**
  - **Vulnerability High (UHF protocol, no encryption)**

→ **Risk Value 5/8**

Signage (EN 16570)

ISO/IEC 29160 : RFID Emblem



Additional Information to be provided by RFID operators

NFC tags may be read in this area for the purpose of easy NFC Smartphone based professional data exchanges. vCard application is available on demand and can be embedded in your visitor badge.

vCard application is operated and controlled by French RFID National Center (CNRFID)
A Privacy Impact Assessment has been undertaken and validated by the French Data Protection Authority (CNIL)

PIA summary can be downloaded at
www.centrenational-rfid.com
For more information, please contact us by phone or email:
+33 494 370 937, contact@centrenational-rfid.com

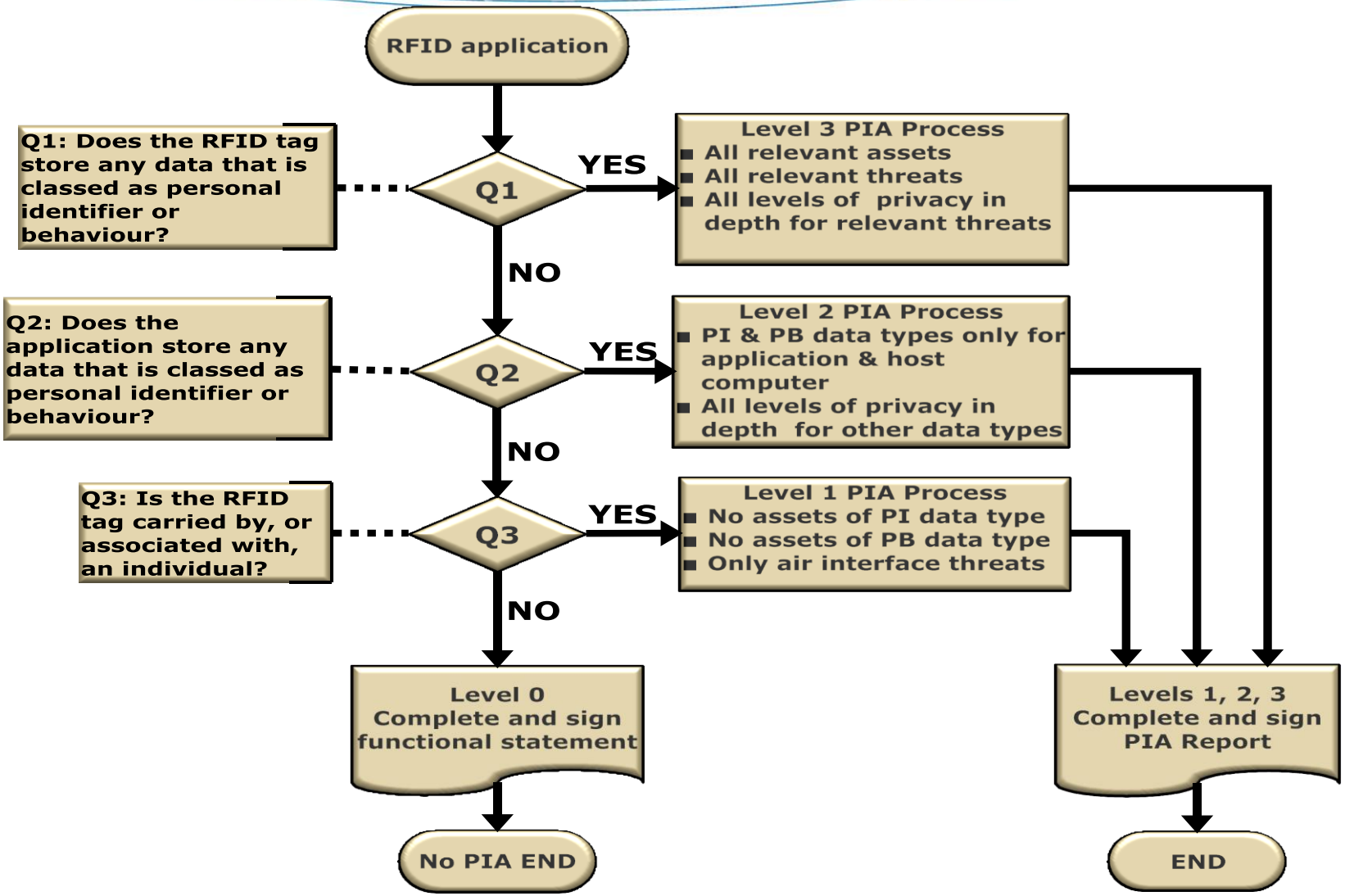
Conclusion

- ✓ **RFID operators have now all the reference texts to undertake a PIA**
- ✓ **PIA is a good practice and is not mandatory**
  - ➢ **European Recommendation**
  - ➢ **Next step: European Regulation ? All ICT technologies will be covered**
- ✓ **PIA is a good way to establish trust between operators and citizen**
- ✓ **PIA approach could be spread to other communication and internet technologies**
- ✓ **Governments could be a forerunner with ID applications…**

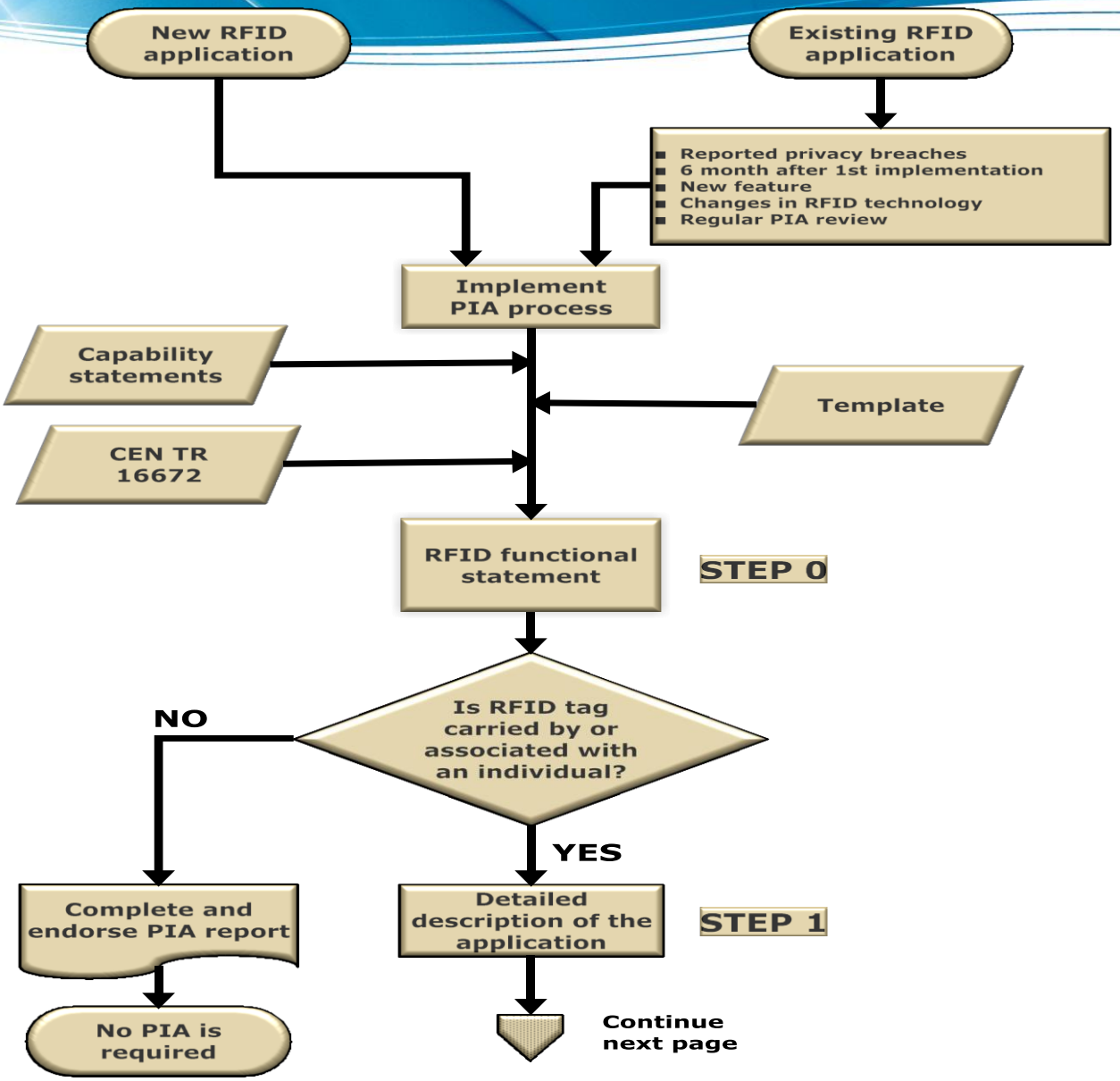
Conclusion

Thank you for your attention

Assess the PIA level



PIA flowchart (EN 16571)



PIA flowchart (EN 16571)