CNRFID
CENTRE NATIONAL
DE REFERENCE

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

RFID, un tour d'horizon technologique, normatif et applicatif

Claude Tételin
Directeur Technique
Président AFNOR CN31

24 Septembre 2013

Sommaire

- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

Le CNRFID

Le CNRFID, Une Initiative Nationale

- Initié par le Ministère de l'Industrie et des Finances
- Créé par le Pôle de compétitivité Solutions Communicantes Sécurisées et le Pôle Traçabilité en juillet 2008
- Mis en place opérationnellement en janvier 2009

Association loi 1901, cofinancée par :

- L'Etat (DGCIS)
- Ses adhérents
- Ses services

Une expertise reconnue :

- Membre des comités de normalisation internationaux (CEN, ETSI, ISO)
- Présidences & vice présidences
- Mandat européen, « Privacy & Public Awarness », Présidence groupe norme liées au processus PIA

Nos valeurs

- **Indépendance**

  Association indépendante de tout organisme, secteur, profession, marché ou région

- **Transparence et neutralité**

  Le CNRFID a pour mission de promouvoir l'utilisation intelligente des technologies RFID et NFC. Cette mission est menée dans la plus grande transparence et avec toute la neutralité et confidentialité qui s'impose à un Centre National de Référence.

Notre Mission

1. **Accompagner le développement** (financièrement et techniquement) des solutions sans contact
2. Contribuer à la **normalisation**, aux évolutions légales et règlementaires
3. Favoriser le **développement d'une synergie stratégique et opérationnelle** de nos adhérents offreurs et utilisateurs au niveau national, européen et international
4. **Former et informer** les utilisateurs/offreurs de solutions sans contact
5. **Répertorier** les **solutions technologiques**

Des adhérents représentatifs de la chaîne de valeur de la RFID

LES UTILISATEURS

ARJOWIGGINS GRAPHIC · Carrefour · castorama · cache cache · CLEOR · DASSAULT AVIATION · DEVANLAY · DIAM INTERNATIONAL · DOMAINE CLARENCE DILLON SAS · EDF · EFS · ERDF · EURO DISNEYLAND PARIS · GDF SUEZ · GEODIS · markem-imaje · MEDINORME · NUTSET · PREMIUMPROTECTOR · RATP · RENAULT · Thélim · TOTAL

LES ACADÉMIQUES (UNIVERSITÉS, LABORATOIRES, CENTRES DE RECHERCHE)

Aix-Marseille Université · cea · cnrs · ETSI World Class Standards · ESEO · Inria · ISEN école d'ingénieurs · LNE

LES AUTRES PARTENAIRES

CNR SANTÉ · filrfid · GS1 France · Hospitalia · NET7 · Pôle de compétitivité Industries du Commerce · Reed Expositions · RFID

LES OFFREURS

Add.Sap · AGID · APROGSYS · ARaymond · ATLANTIC RF · AXEM Technology · BEWETS · biolog-id · CASSIDIAN · CCRM · CDVI · CIPAM · CSC · deister electronic · dmph consulting · EBV · EMBISPHERE · EMITECH · etikQuest · FIME · frequentiel · GEMA CONSULT · GENESINK · HID · HMY · Hub One · I3S-SOLUTIONS · idem · iER · ifm electronic · Insight SP · Jidélec · MAINtag · neopost · Nexess · NORCOD · NORDICID · NRF LAB · ORIDAO · P3 · page up · PRAGMATIK · RFIDEAL · RFID Labs · Schneider Electric · sieve · SOLEM · STid · Systerel · TAGEOS · TAGPLAY · TAG PRODUCT · TAGSYS RFID · Twister · Ubisense

Puce électronique → Etiquette, Tag, carte → Interrogateur → Packaging, Capteurs, Sécurité → Software, Réseau → Intégration → Utilisateur final

Les actions du CNRFID

Evénements et rencontres business

Accompagnement Projet

Le soutien aux PME

Norme, règlementation et standardisation

Services du CNRFID

Formations et Informations

Veille technologique et stratégique

Implication au sein de l'univers académique

Sommaire

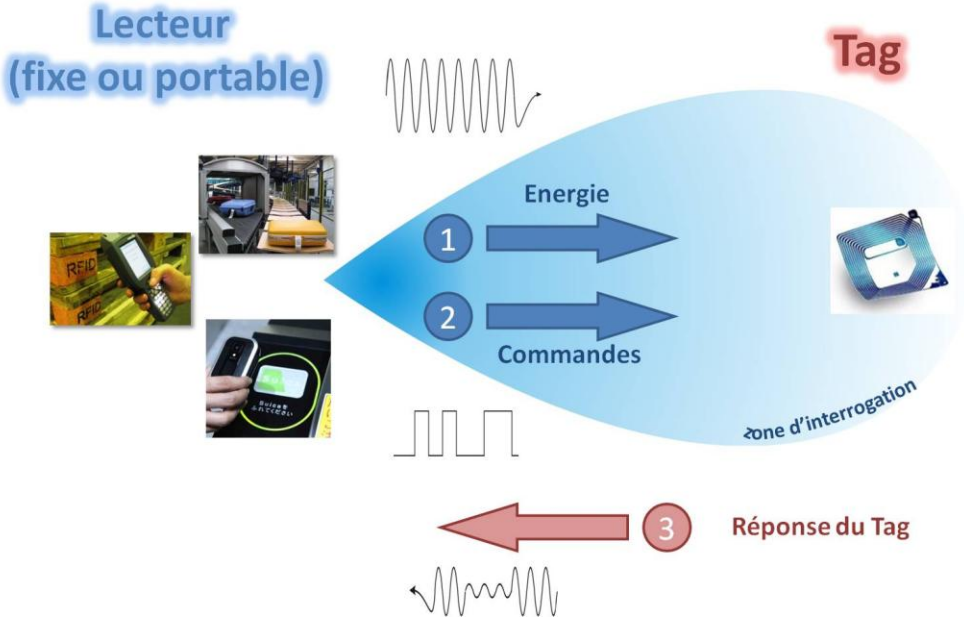
- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

Classification de la RFID

Définition de la RFID :

Technologie d'**identification automatique** utilisant le rayonnement **radiofréquence** pour identifier des objets porteurs d'**étiquettes** lorsqu'ils passent à proximité d'un **interrogateur**.

Ce dernier transfère les données contenues dans la puce de l'étiquette vers l'interrogateur, ou les modifie suite à une commande particulière.



Classification de la RFID

TAG

ANTENNE

INTERFACE

AIR

DONNES

ENERGIE

ANTENNE

LECTEUR

MIDDLEWARE

APPLICATIFS METIERS

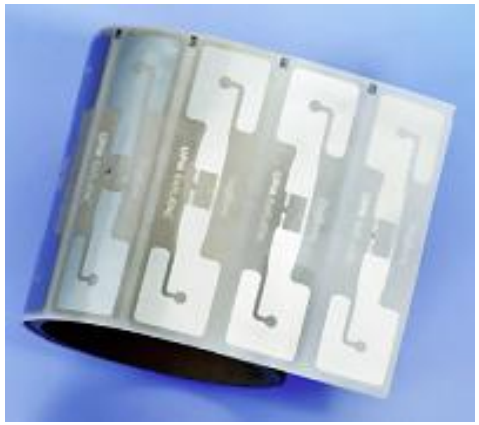
UTILISATEURS

Classification de la RFID

- **Actif / Passif / Battery Assisted**
- **Actif** : la puce possède son propre émetteur RF
  - Plus complexe donc plus cher
  - Meilleures portées (> 100 m)
  - Nécessite une source d'énergie dans le tag
- **Passif** : la puce n'a pas d'émetteur RF à bord
  - Faible coût
  - Communication par rétro modulation ou backscattering
  - Portée réduite à 10 m maximum
  - Alimentation par couplage RF avec l'interrogateur
- **Battery Assisted** : du passif mais avec une batterie
  - Communique comme le passif (portées équivalentes)
  - Possède une batterie pour alimenter un périphérique (généralement de type capteur)

Classification de la RFID

- **Couplages lecteur/tag ou Fréquences**
- **Couplage Inductif** : le champ magnétique est prépondérant
  - Systèmes LF (125kHz) ou HF (13,56MHz)
  - Antennes = Boucles
  - Diminution rapide des champs = zone d'interrogation clairement définie



- **Couplage propagatif** : le champ électromagnétique est formé
  - Systèmes UHF (433 et 860-960MHz) et SHF (2,45GHz)
  - Antennes = Dipôles
  - Propagation = réflexions et diffractions = zones d'ombre possibles

Classification de la RFID

- **Types et taille mémoire**
- **Read Only**
  - L'utilisateur n'a pas la main sur l'information contenue dans cette zone
  - TID : Tag Identifier (32 ou 64 bits en général)
  - Gravé par le fondeur de la puce
- **Write Once Read Multiple**
  - L'utilisateur peut encoder 1 fois et une seule
  - UII : Unique Item Identifier (32, 64, 96 ou 128 bits)
  - Code EPC (GS1)
- **Multi Time Programmable** : User Memory
  - Quelques bits à quelques kilobits
  - Possibilité de contrôle d'accès (login, password)
- **Protocoles TTF, RTF, ToTaL**

Classification par marché

Des secteurs à fort potentiel d'utilisation


aéronautique


automobile


grande distribution


industrie


logistique


luxe


santé


textile

Des niches déjà opérationnelles


bibliothèque


blanchisserie

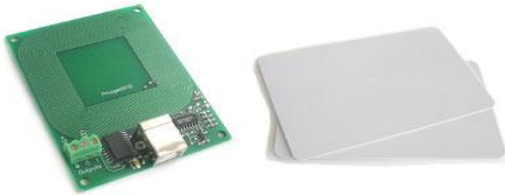

télépéage

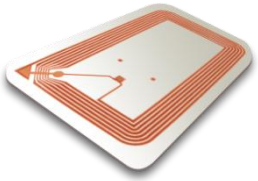
ticketing

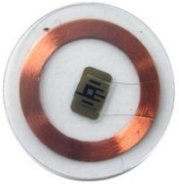
Classification des lecteurs

Classification des lecteurs

Classification des tags





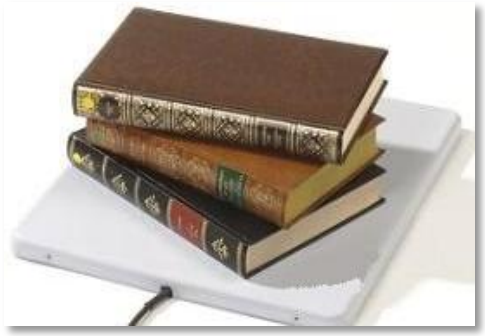


Sommaire

- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

Quand la RFID s'impose …. ou pas

- **Lecture à distance**
  - Du Touch'n Go à plusieurs mètres en passif (>100 m en actif)
  - Mieux vaut parler de volume de lecture plutôt que de distance !
- **Lecture sans visibilité**
  - Propriétés des ondes électromagnétiques
  - Prendre en compte l'environnement (métal, eau, etc.)
- **Lectures simultanées**
  - Jusqu'à 100 tags/s suivant le protocole
  - Adapter le protocole à l'application (pass Navigo vs. Quai de chargement)



Si vous n'avez pas besoin d'au moins une de ces trois propriétés, vous n'avez pas besoin de la RFID

Quand la RFID s'impose …. ou pas

- **Réécriture mémoire**
  - Le tag garde un historique
  - Pas besoin de connexion réseau pour retrouver des informations sur le produit
- **UII long**
  - N bits : 2^N possibilités
  - Chaque item devient unique
- **Packaging adaptés**
  - Pas besoin de visibilité
  - Tag inclus dans le produit
  - Protection contre agressions extérieures
- **Connexion avec périphériques**
  - Tags actifs ou BAP

Sommaire

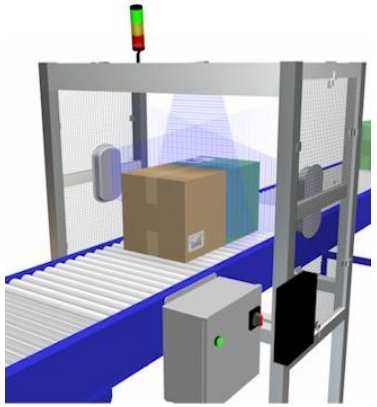
- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

Quelles performances? A quels prix?

- **Lecteur/Interrogateur**
  - Module OEM ou entièrement packagé, portable ou fixe
  - De quelques dizaines d'euros à 1500 euros
  - Prévoir connectique, amplificateur, communication (USB, GPRS, Wifi, Ethernet, etc.), programmation
  - 1 à 4 ports pour antennes
- **Antennes**
  - Toutes technologies : LF, HF, UHF
  - Taille : de quelques cm à plus d'un mètre (influence la distance de communication)
  - De 10 à 500 euros

Quelles performances? A quels prix?

- **Ergonomies**
  - Lecteur mobile (+ raquette) (à partir de 1k€)
  - Lecteur fixe simple
  - Portique (5 à 10 k€)
  - Tunnel (5 à 10 k€)



Quelles performances? A quels prix?

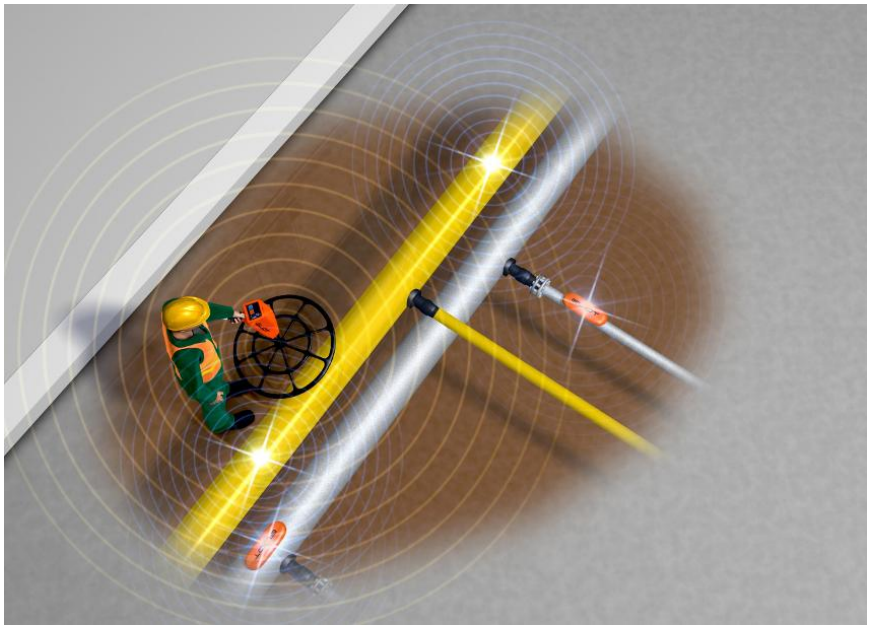
- **Dry/wet inlays**
  - Disponibles en technologie HF et UHF (pas en LF)
  - Min 10cts l'unité (pour 100.000 pièces) UHF, de l'ordre de l'euro par unité pour une puce sécurisée HF
  - Jusqu'à 7 mètres en UHF, 1,5 mètres en HF ou LF
  - Sensible au support
- **Tags packagé**
  - Toutes technologies : LF, HF, UHF
  - De 1 à 10 euros suivant packaging
  - Spécial métal, Hte température, humidité, pression, etc.
- **Tags actifs et BAP**
  - Tags packagés, HF ou UHF
  - À partir de 5 euros en BAP et 10 euros en actif
  - BAP : meilleure distance en écriture que passif (proche de distance de lecture)

Sommaire

- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

Applications et cas d'usages

Détection de réseaux enterrés



Détection des réseaux jusqu'à 1,5 m de profondeur

Applications et cas d'usages

Détection vols sur chantiers

- Création de zones de détection RF autour du chantier.
- Alarmes lorsque sortie de la zone.
- Dissuasion.
- Dissimulation / Protection du tag nécessaire.

Applications et cas d'usages

Suivi sur lignes de productions

- Identification unitaire de véhicules.
- Suivi de véhicules sur lignes de productions.
- Configuration automatique de machines outils.
- Contrôles de passages de véhicules.
- Localisation de véhicules sur parking.

Applications et cas d'usages

Gestion et contrôle de maintenance

Accès en lecture et écriture, quel que soit la couverture réseau, aux informations de maintenance essentielles : date de dernière revue, personne ayant effectué le contrôle…

Applications et cas d'usages

Gestion des petits outillages

- Armoires, servantes, et tables de magasins intelligents.
- Détection RFID jusqu'à 1m.

Applications et cas d'usages

Suivi et localisation de pièces et gros outillages

Localisation obtenue par
triangulation de signaux RFID actifs

Applications et cas d'usages

Suivi de contenants

Suivi de palettes sur plateforme logistique DHL pour Métro

Suivi des 600 000 bacs de fruits et légume Auchan

Suivi des bacs de médicaments, plateforme pharmaceutique CERP

Applications et cas d'usages

Couplage capteurs

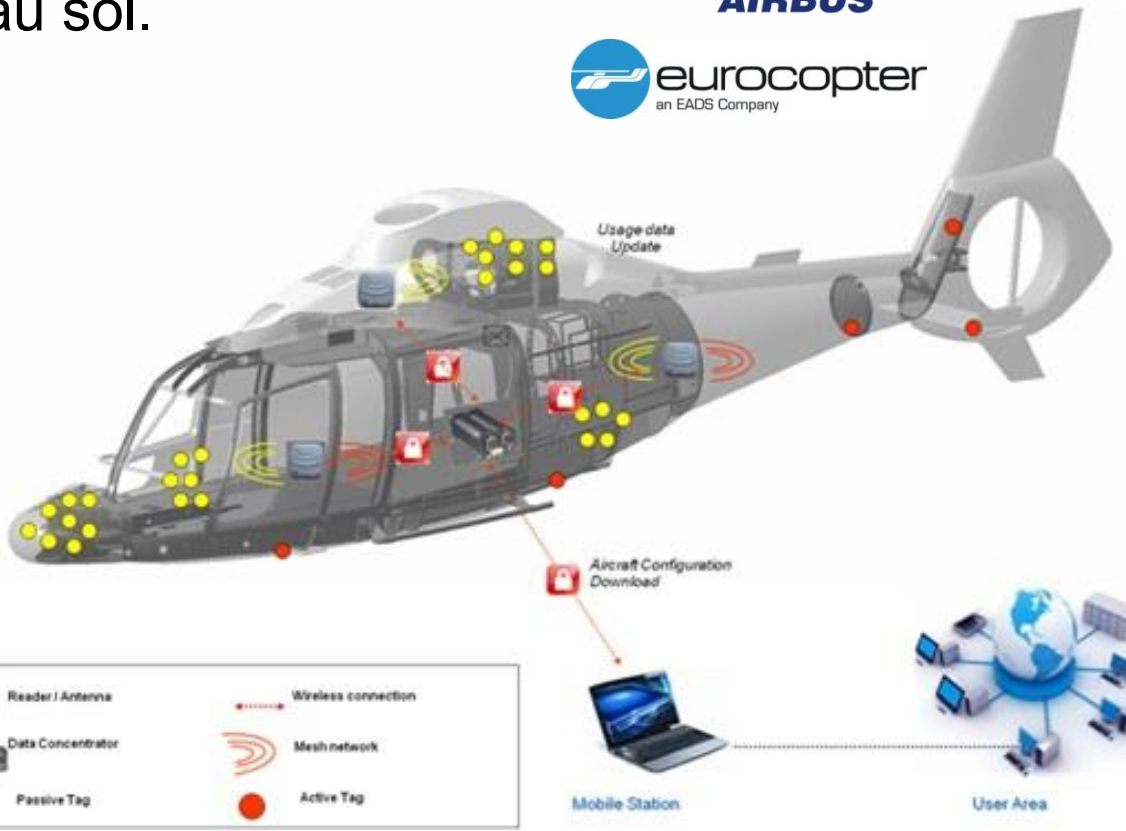
Couplage tags RFID –
Capteurs divers : température, choc, humidité, luminosité…

EFS
ÉTABLISSEMENT FRANÇAIS DU SANG

Applications et cas d'usages

Contrôle de présence d'équipement embarqués

- Suivi et contrôle d'équipements embarqués.
- Traçabilité d'outillages au sol.



Applications et cas d'usages

Contrôle d'accès, transport et paiement

- Technologie LF ou HF
- Applications sécurisées
- Pas d'anticollision

Applications et cas d'usages

Bibliothèques

- Technologie HF standardisée (ISO 28560)
- Contrôles E/S, Inventaires, Information au public
- Percée de l'UHF…

Applications et cas d'usages

Textile

- Historiquement HF mais de + en + souvent UHF
- Faibles contraintes environnementales
- Largement répandu pour laveries industrielles (hôpitaux, hôtels, agro-alimentaire, etc.)
- Fait son apparition dans certaines enseignes (Décathlon, Gerry Webber, Macy's, Maks and Spencer…)
- Couplage avec anti-vol (techno UHF)

Applications et cas d'usages

Convergence UHF/HF

- HF – Sécurité, UHF - longe distance
- HF – NFC (info consommateur), UHF - logistique
- Tags bi-fréquence
- Lecteurs bi-fréquence
- Smartphone NFC + UHF
- EPC Global (encodage identique HF/UHF)
- Problème du coût
- Problème des interférences

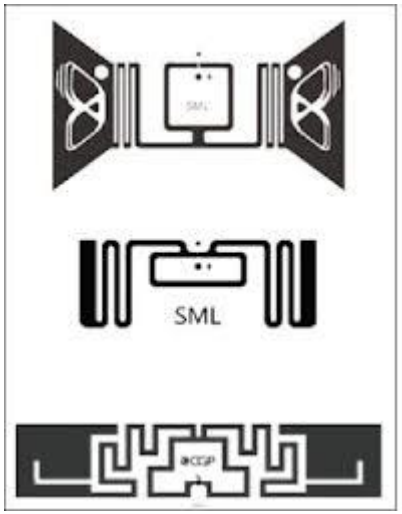
Sommaire

- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage et la sécurité
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

Encodage

- Memory
- Unique Identifiers and co.
- UII, TID, EPC and other vocabulary issues
- Global representation of RFID system and related standards
- TID and ISO 15963
- Focus on ISO 15693 (HF vicinity smartcards)
- Focus on ISO 18000-63 and EPC Class1 Gen2 (UHF RFID)

Memory



- **RFID chips only use non volatile memory** (because RFID tags have to store information even when they are not powered)
- **RFID chips mainly use EEPROM technology because:**
  - **the size of the memory do not exceed tens of kbytes**
  - **each bit of memory can be addressed individually** (no need to lose time and energy to write complete blocks even if it is sometimes possible)
  - **EEPROM is a stable technology** (lower cost)
- **FeRAM are used for applications which require high capacity memory** (Fujitsu UHF tag with up to 64 kbytes user memory)

Identifiants uniques

- **Identifier:**

  Part of the chip's memory to (uniquely) identify: the chip itself, the tag or the object to which the tag will be attached

  Could be use for anticollision process

- **Questions:**
  - What should be the length of an identifier?
  - Where should this information be placed in the memory?
  - Should this information be unique?
  - Could this information be changed?
  - Who could certify the uniqueness of the identifier?

Identifiants uniques

- **Identifier length:** $n \ bits \Rightarrow 2^n \ possibilites$

$$2^{50} = 1\,125\,899\,906\,842\,624 \approx 1{,}12 \ \ 10^{15}$$

- With 50 bits, we can count individually all the grain of sand of all the beach on earth

$$2^{96} = 79\,228\,162\,514\,264\,337\,593\,543\,950\,336 \approx 7{,}9 \ \ 10^{28}$$

- With 96 bits, we can count all single rice grain produced on earth for the next 8000 billion years…

Identifiants uniques

- **Protection features:**
  - None: everyone can read/erase/write at the identifier memory location

  - Lock: Once written by an authorized organization, the identifier is locked. Everyone can read it but need a password to change it. Questions:
    - What is an authorized organization?
    - Who define the password and store it?
    - Is there a different password for each tag?

  - PermaLock: Once written by an authorized organization, the identifier is permanently locked. Everyone can read it but identifier can never been changed again.
    - Be careful when permalocking an encoded identifier
    - Un-permalocking of tag is sometimes possible but very difficult (recommissioning)

Identifiants uniques

- **Uniqueness of the identifier:**
  - Close Loop application: need to have unique identifiers inside the application. The operator can assign identifiers himself. He can use is own identifier format (eg. 10 bits long, 5 MSB for part number, 5 LSB for serial number)

  - Open Loop application: tags are used across a given process and shared by different stakeholders.
    - identifiers have to be unique: rules have to be set up to create and handle them
    - memory location has to be standardized
    - encoding rules have to be shared across the application
    - need for a Registration Authority (application leader, federation, third party,…)

CNRFID
CENTRE NATIONAL
DE REFERENCE

Acronymes

- **CID: Chip Identifier**

  Number used to identify the chip. Usually encoded by the chip manufacturer in a ROM like memory. Cf. TID

- **TID: Tag Identifier**

  Number used to identify a RFID Tag. Usually encoded by the tag manufacturer or chip manufacturer in a ROM like memory. Manufacturers may use the ISO 15963 encoding rules.

- **UII/UID: Unique Item Identifier/Unique Identifier**

  UII is a code that identifies the object to which a tag is affixed. For ISO applications, UII has to follow ISO 15962

- **EPC: Electronic Product Code**

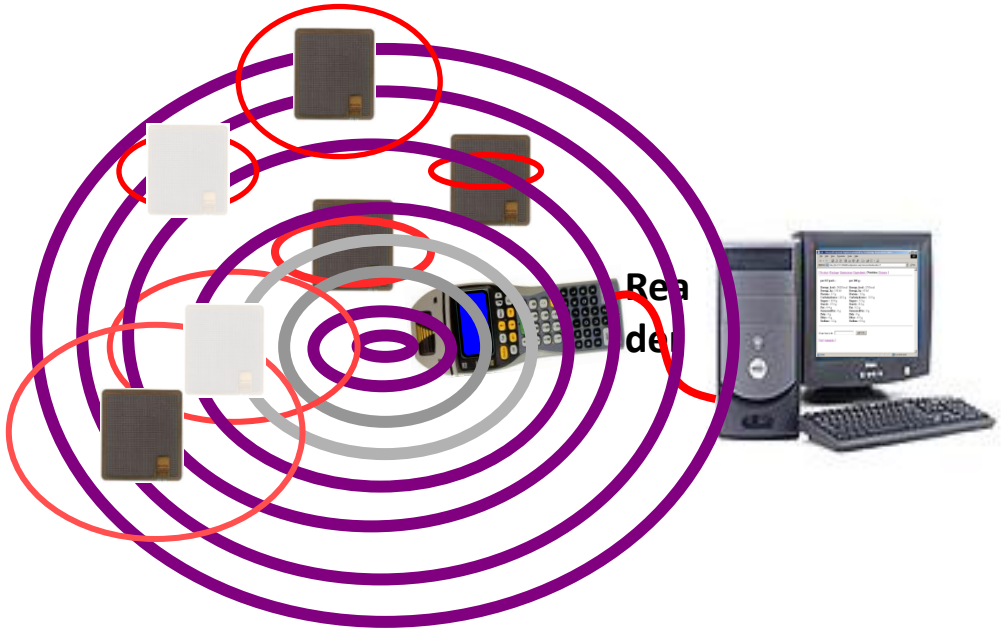
  EPC is a special case of UII and is proposed by GS1. For EPCGlobal applications, UII (EPC) has to follow EPCglobal Tag Data Standards.

Acronymes

- **AFI: Application Family Identifier**

  AFI represents the type of application targeted by the RFID readers and is used to extract from all the RFID tags present only the tags meeting the required application criteria. AFI is defined in ISO/IEC 15961-3

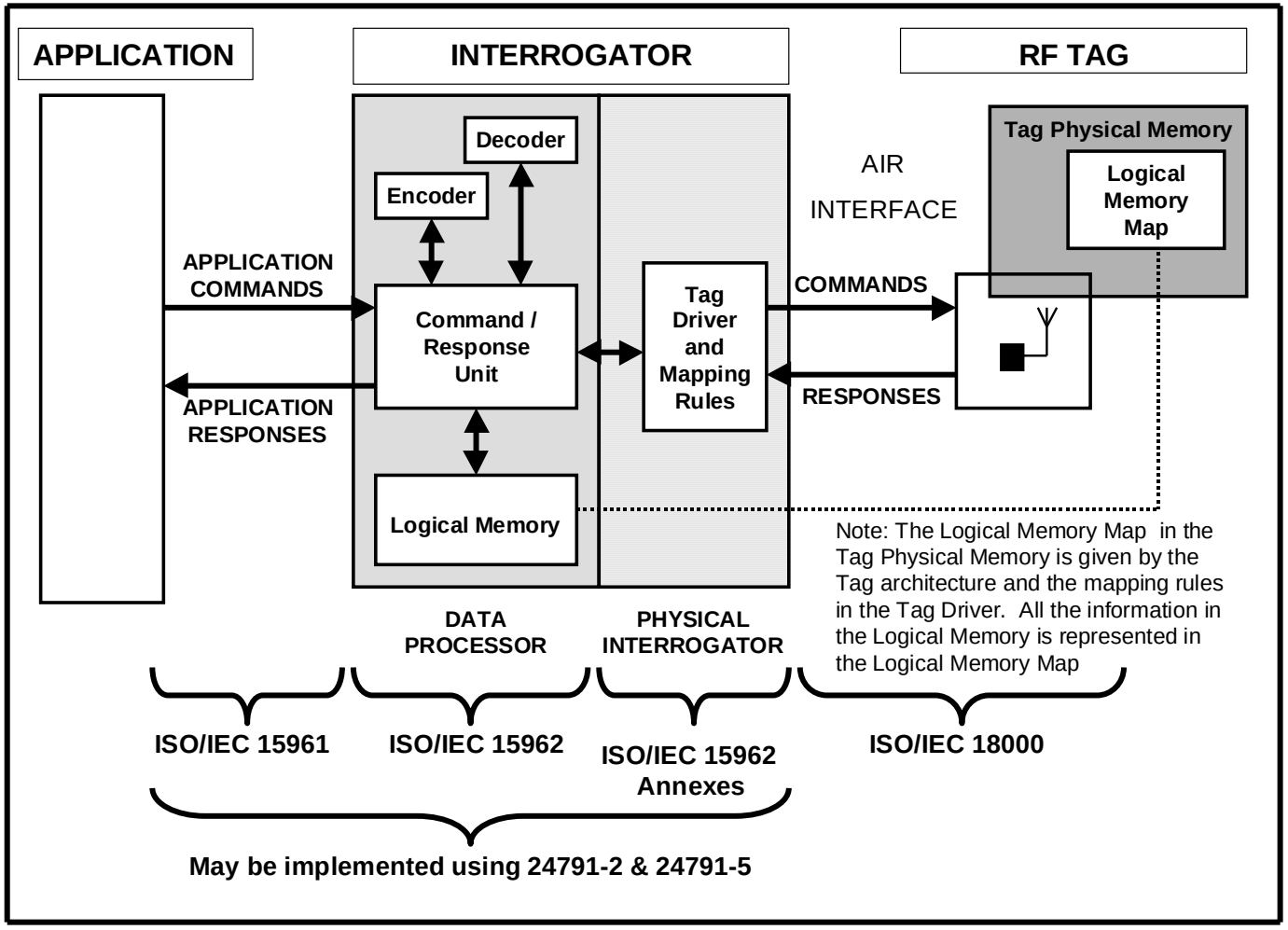
  AFI is also used for contactless smartcards applications (banking, transport, access control, etc.). AFI codes are defined by ISO 14443 and ISO 15693
  AFI is a powerful tool to speed up anti-collision process



Courtesy of Paul Chartier, Praxis Consultants

Global representation of RFID system

- ISO based structure



Global representation of RFID system

- **ISO based structure**

The Data Protocol addresses data handling between the application and the RF tag

ISO/IEC 15961 Data protocol - application interface:

defines the application commands and responses
uses object identifiers to define all data types

ISO/IEC 15962 Data protocol - data encoding rules

efficient encoding of object identifiers
common data compaction

Global representation of RFID system

- **ISO based structure**

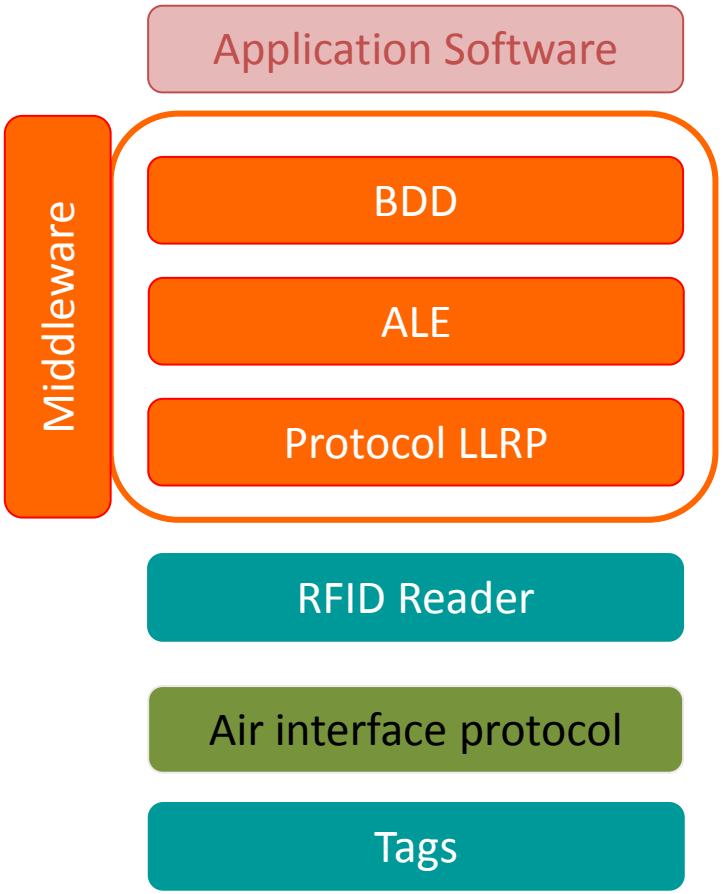
ISO/IEC 24791-2 Software system infrastructure: Data management
defines the interface(s) that provide **operations on RFID tag data including reading, writing, collection, filtering, grouping, and event subscription and notification** within the Software System Infrastructure

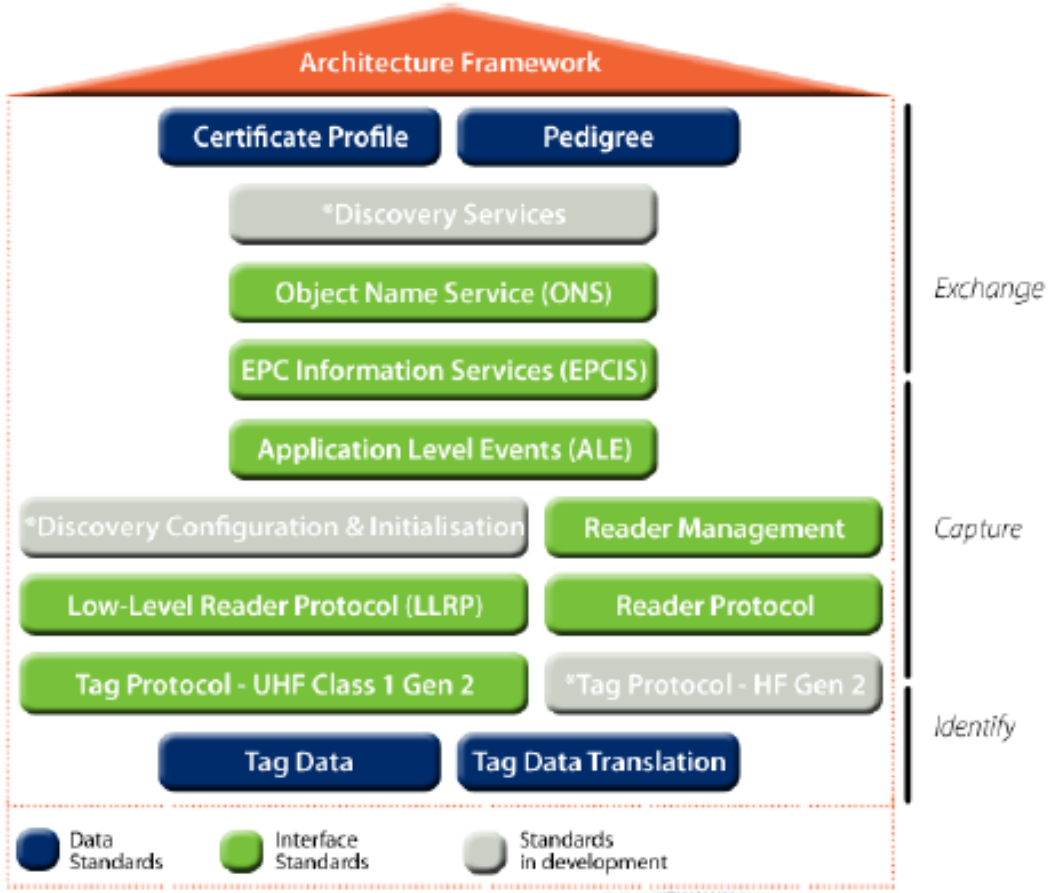
ISO/IEC 24791-5 Software system infrastructure: Device interface
defines an interface within the Software System Infrastructure (SSI) that provides RFID system control components with **low-level access to RFID interrogators for the purpose of optimizing RFID data access and control operations**

Note1: The 2012 version only supports ISO 18000-6 typeC air interface
Note2: equivalent to EPCGlobal LLRP standard

Global representation of RFID system

- **GS1 EPC Global based structure**

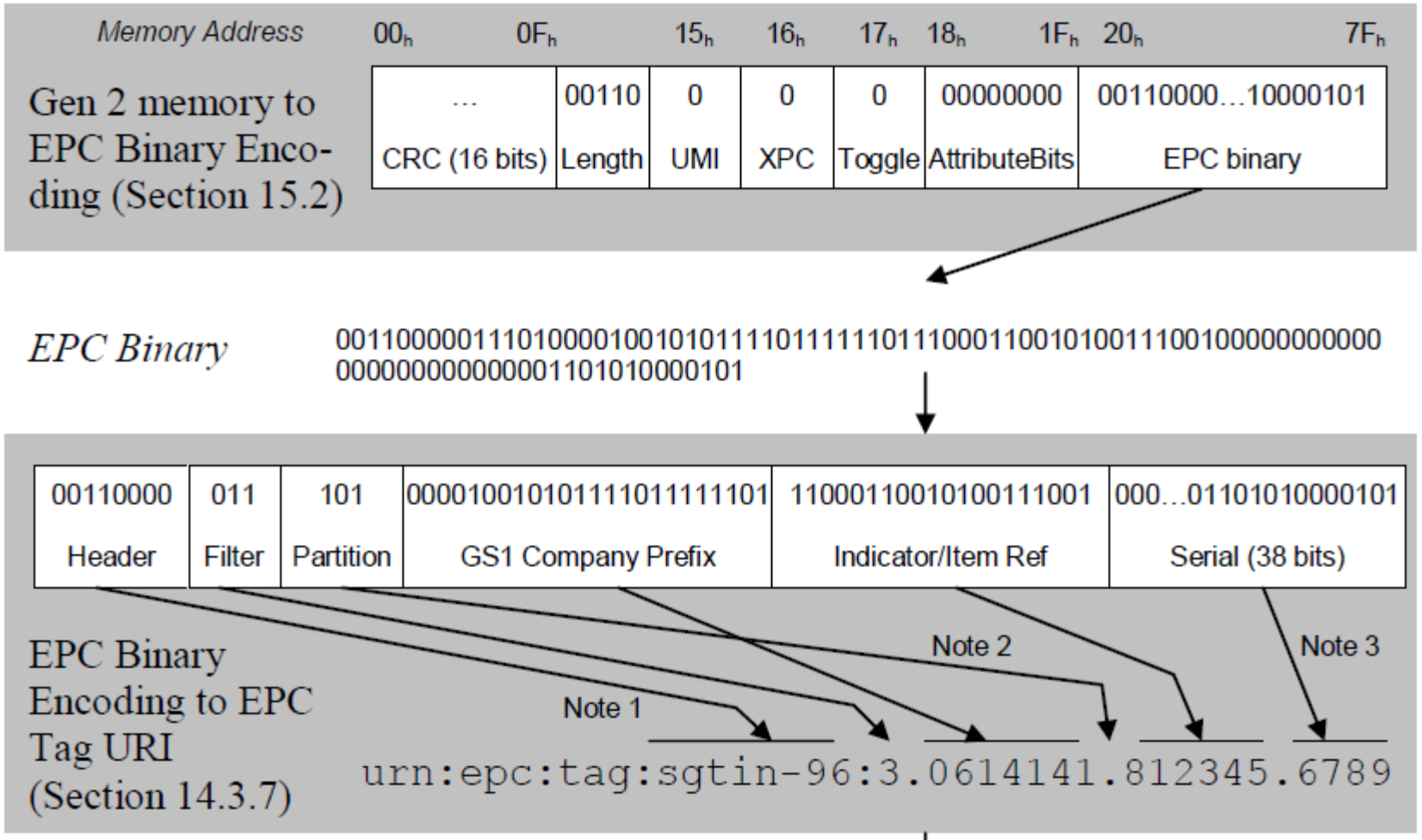




Global representation of RFID system

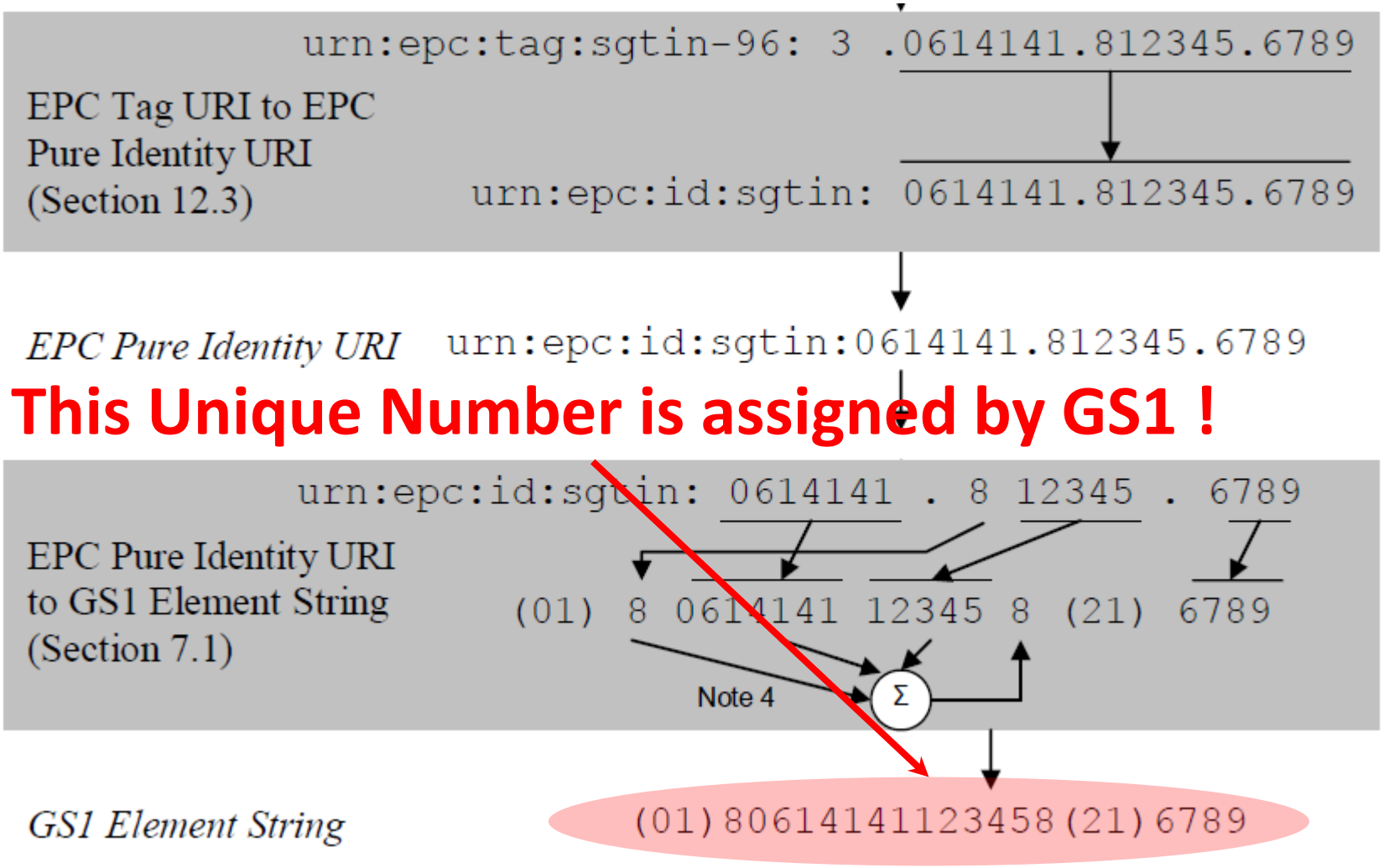
- **EPCGlobal based structure**

  Everything is based on EPC code and EPC memory bank



Global representation of RFID system

- **EPCGlobal based structure**



Example of ISO 15693

- **ISO 15693 is a HF (13,56 MHz) air-interface standard developed by SC17**
- **Mainly used for item identification and libraries**
- **Reading distance: up to 1,5m**
- **Two different types (A & B, Long range / Fast rate)**
- **Communication to card**
    - **1 out of 4 pulse position modulation**

      2 bits are coded as the position of a 9.44 µs pause in a 75.52 µs symbol time, giving a bit rate of 26.48 kb/s
    - **1 out of 256 pulse position modulation**

      8 bits are coded as the position of a 9.44 µs pause in a 4.833 ms symbol time, giving a bit rate of 1.65 kbit/s

Example of ISO 15693

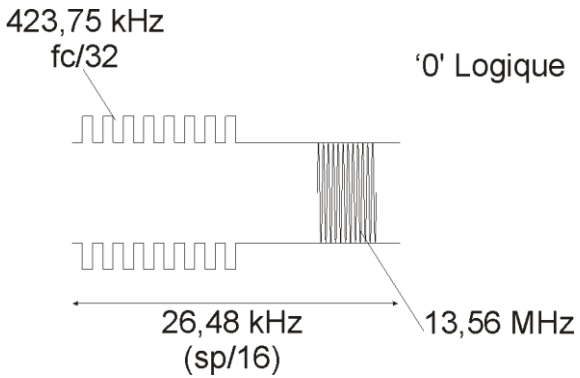
- **Communication to reader**

Low 6.62 kbit/s (fc/2048) or High 26.48 kbit/s (fc/512)

Manchester Coding

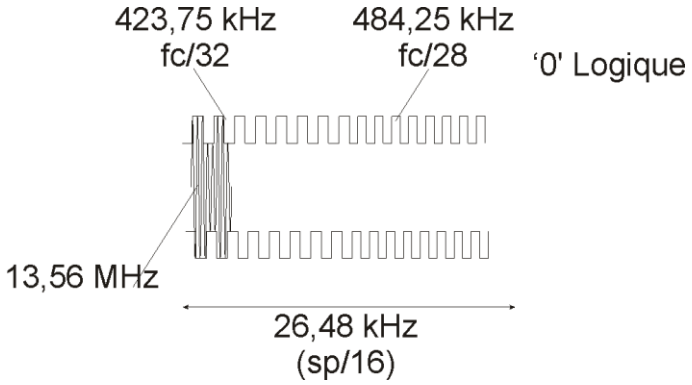
- **Amplitude Shift Keying**

100% modulation index on a 423.75 kHz subcarrier



- **Frequency shift keying**

2 subcarriers: 423,75 kHz (fc/32) and 484.25 kHz (fc/28)



Example of ISO 15693

- **TID (also called UID in the standard)**
  - VICCs are uniquely identified by a **64 bits unique identifier**

MSB LSB

64 57	56 49	48 1
'E0'	IC Mfg code	IC manufacturer serial number

  - The 8 MSB bits shall be 'E0'
  - IC manufacturer code, on 8 bits according to ISO/IEC 7816-6/AM1
  - A unique serial number on 48 bits assigned by the IC manufacturer

Example of ISO 15693

- **AFI (Application Family Identifier)**
  - Coded on 1 byte (2 x 4 bits)

Table 1 — AFI coding

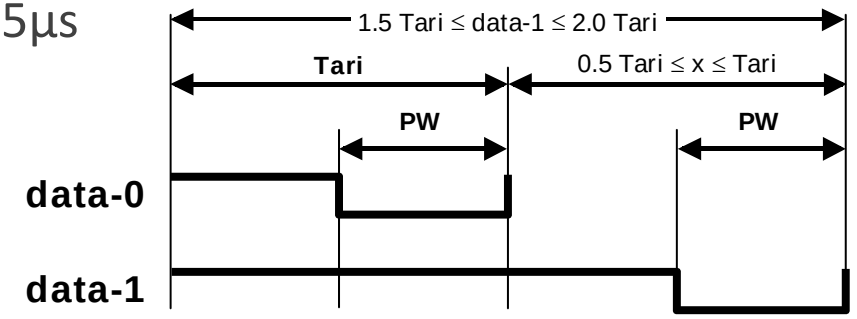
AFI most significant nibble	AFI least significant nibble	Meaning VICCs respond from	Examples / note
'0'	'0'	All families and sub-families	No applicative preselection
X	'0'	All sub-families of family X	Wide applicative preselection
X	Y	Only the Yth sub-family of family X	
'0'	Y	Proprietary sub-family Y only	
'1'	'0', Y	Transport	Mass transit, Bus, Airline
'2'	'0', Y	Financial	IEP, Banking, Retail
'3'	'0', Y	Identification	Access control
'4'	'0', Y	Telecommunication	Public telephony, GSM
'5'	'0', Y	Medical	

Example of ISO 15693

- **Memory organization**
  - Up to 256 blocks can be addressed
  - Block size up to 256 bits
  - Maximum capacity of 8kbytes (64 kbits)
  - Possible NWIP from 2 vendors for higher memory capacity and security features
- **ISO 15693 is the base of ISO 18000-3 mode 1**
- **ISO 18000-3 mode 3 is the “equivalent” of the EPC Class1 HF**

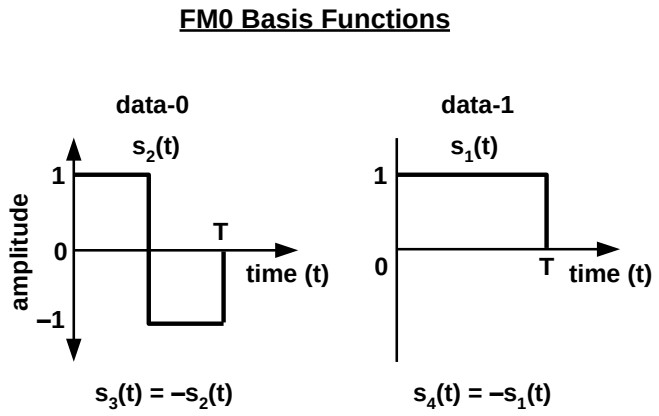
Example of ISO 18000-63

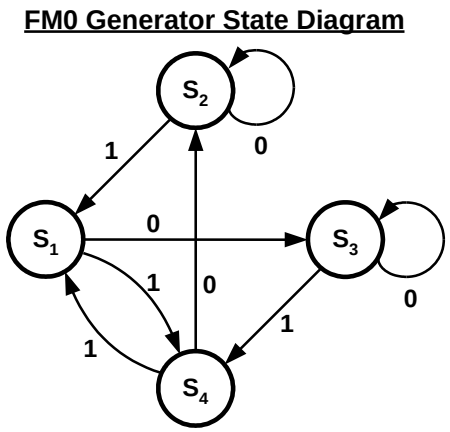
- **ISO 18000-63 is a UHF (860-960 MHz) air-interface standard developed by SC31**
- **“Equivalent” to ISO 18000-6 type C and EPC Class1 Gen2 for item identification**
- **Reading distance: up to 10m (for passive tags)**
- **Communication reader to tags**
  - DSB – ASK or SSB – ASK or PR – ASK (90% nominal)
  - PIE encoding
  - Bit rate: 26.7 kbit/s to 128 kbit/s (assuming equiprobable data)
  - Tari values between 6.25µs to 25µs



Example of ISO 18000-63

- **Communication tag to reader**
  - Backscaterring
  - ASK or PSK modulation
  - Data encoding: FM0 baseband or Miller modulation of a subcarrier





Example of ISO 18000-63

- **Communication tag to reader**
  - Subcarriers: 40 kHz to 640 kHz
  - Bit rate:
    - FMO: 40 kbps to 640 kbps
    - Miller: 5 kbps to 320 kbps

Example of ISO 18000-63

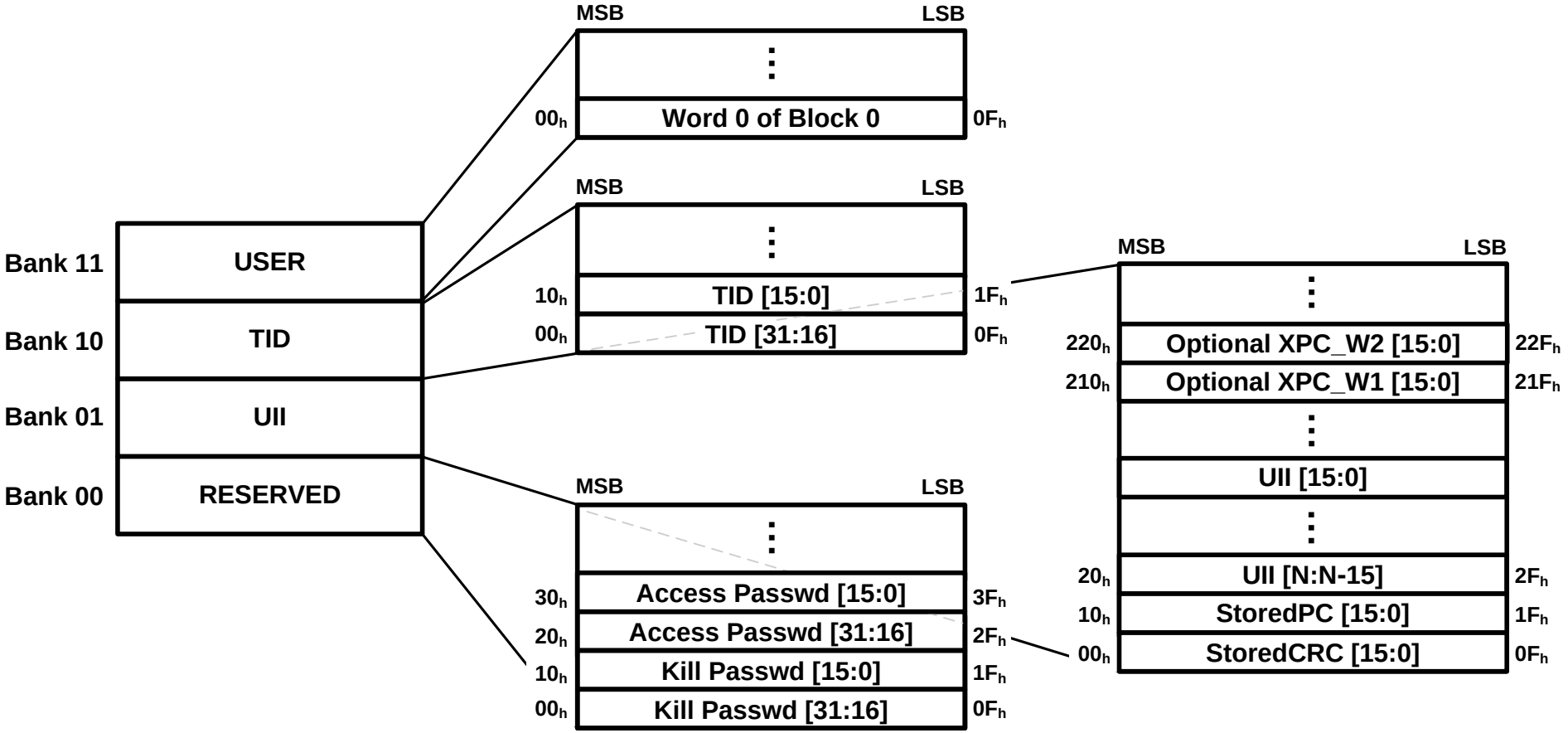
- **Tag memory organization**
  - 4 logical memory banks
  - Reserved memory:
    - kill password shall be stored at memory addresses 00h to 1Fh
      - 32-bit “Kill” password allows a Tag to be permanently silenced
      - The default Kill password value is zero
      - The Kill command will only execute if the password has been set, i.e. is non-zero
    - access password shall be stored at memory addresses 20h to 3Fh

Example of ISO 18000-63

- UII memory:
  - StoredCRC at memory addresses 00h to 0Fh
  - StoredPC at addresses 10h to 1Fh
  - UII beginning at address 20h
  - XPC_W1 and XPC_W2 (if any) beginning at address 210h
- TID memory:
  - 8-bit ISO/IEC 15963 allocation class identifier at memory locations 00h to 07h
  - information above 07h for an Interrogator to uniquely identify the custom commands and/or optional features that a tag supports
- User memory: Optional

Example of ISO 18000-63

- Tag memory organization



Sommaire

- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

La sécurité

1. DICP (disponibilité, intégrité, confidentialité, preuve)
2. Evaluation des risques
3. Les différentes attaques
4. Les contre mesures existantes
5. La cryptographie

La sécurité

- **Disponibilité** :

Garantir le fonctionnement des outils pour la continuité des services aux utilisateurs ;

- **Intégrité** :

Mise à disposition de données de qualité dans les temps et espaces prévus ;

- **Confidentialité** :

Offrir un niveau satisfaisant d'accès et de préservation des données sensibles ;

- **Preuve** :

Garantir la traçabilité suffisante pour tout contrôle.

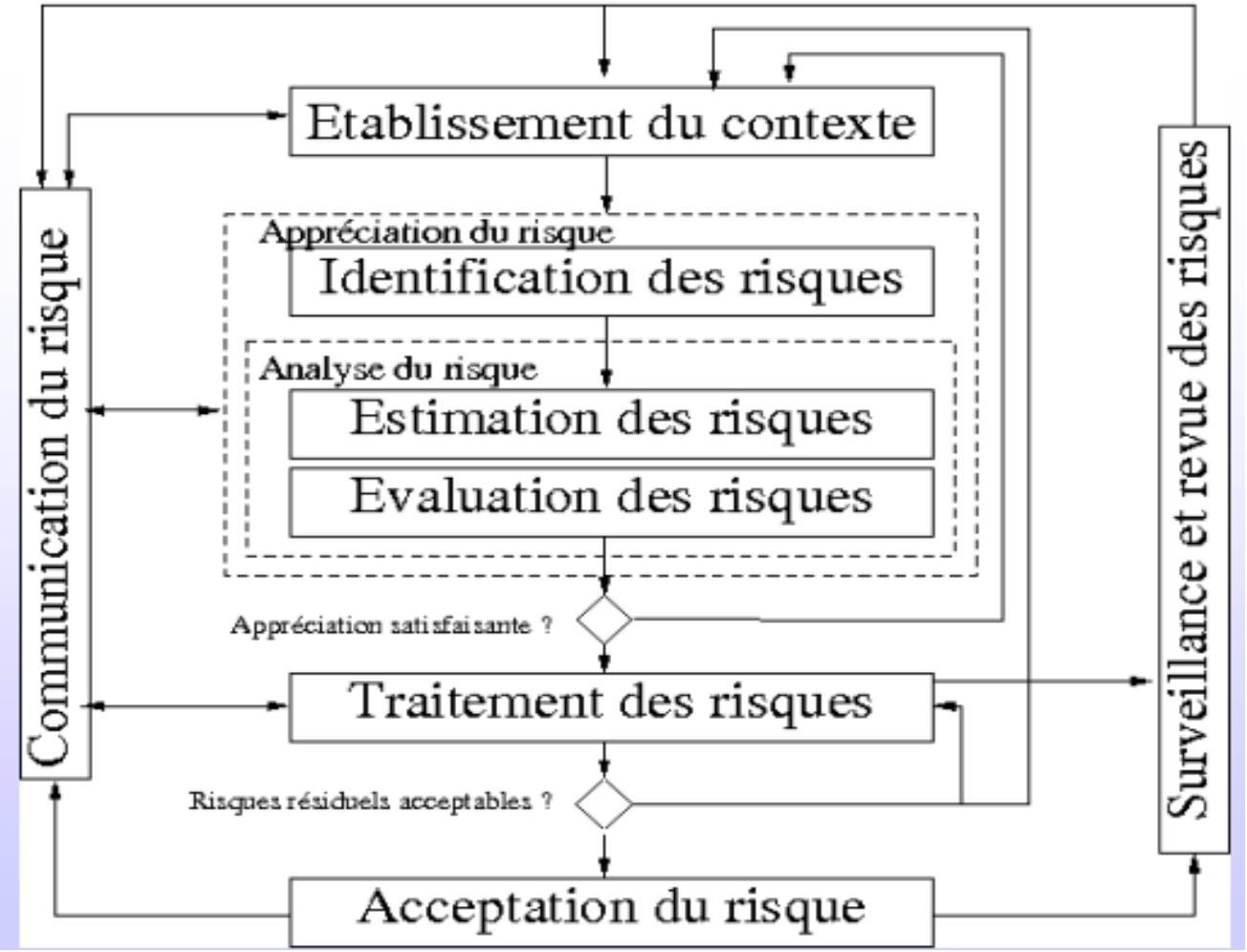
Chacun de ces 4 critères représente des fondamentaux notamment pour assurer la continuité de la communication et de la diffusion des informations confidentielles.

La sécurité

Evaluation des risques

- Quelle serait l'ampleur du dommage si la vulnérabilité était exploitée ?
- L'attaque est-elle facile à reproduire ?
- Est-il facile de lancer une attaque?
- Combien d'utilisateurs seraient concernés ?
- Est-il facile de détecter la vulnérabilité ?

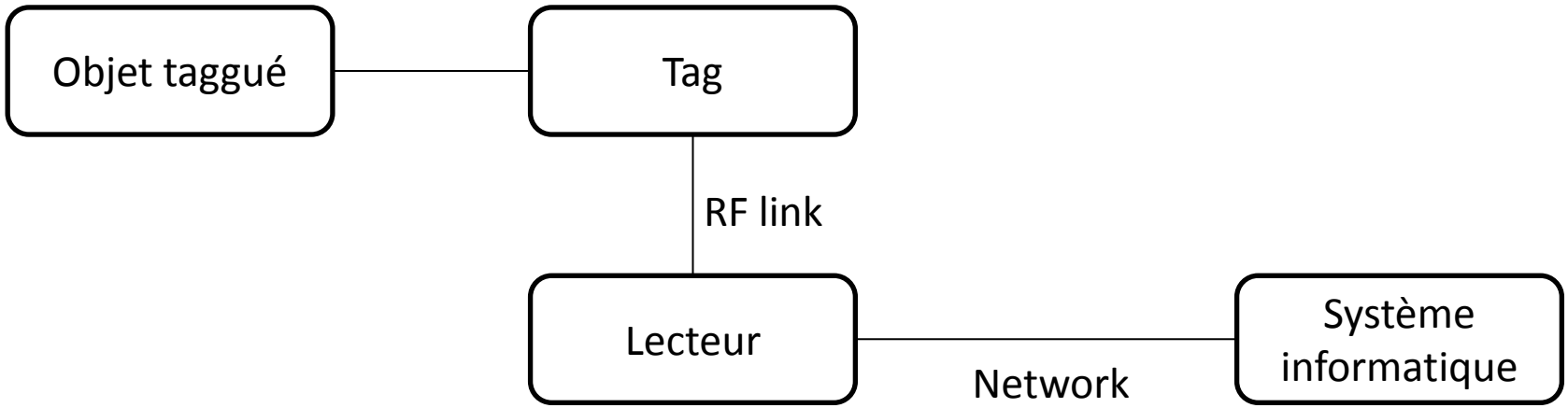
Processus ISO 27005



Les différentes attaques

Les cibles des attaques sont :

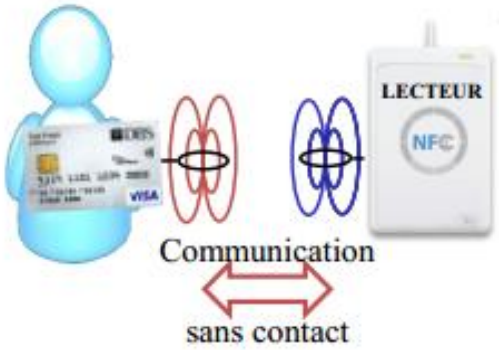
- La puce
- Le lien RF
- Le système de gestion informatique



Attaques RF

- **"Eavesdropping" or “sniffing” (écoute à distance)**

L’attaque « Eavesdropping » permet de surveiller et d’écouter la conversation entre un tag et un lecteur. C’est l’attaque la plus simple à réaliser car elle nécessite peu de matériel.



Attaques RF

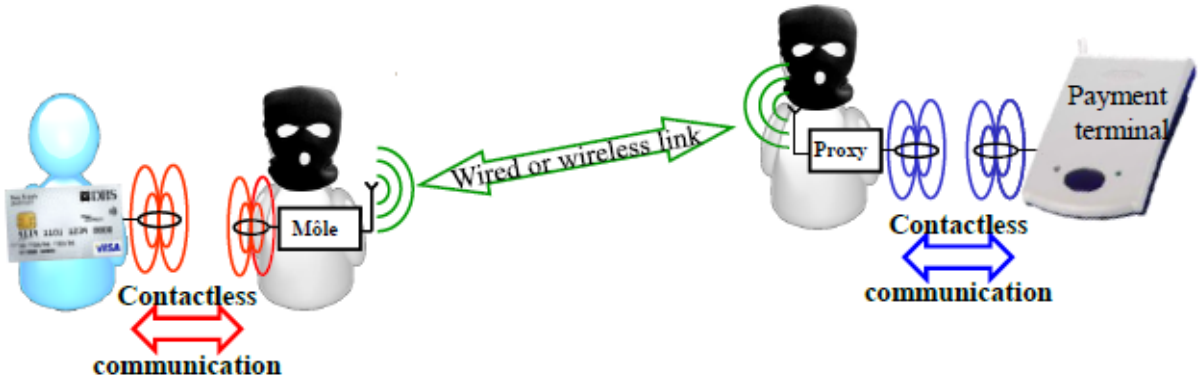
- **Skimming data (activation à distance)**

L'attaque «Skimming data» consiste à récupérer de façon frauduleuse et discrète les informations contenues dans le tag (UID, données à caractère personnel, …).

Attaques RF

- **L'attaque relais**

L'objectif de l'attaque relais consiste à établir une communication entre un lecteur et un tag sans le consentement de son propriétaire. La distance entre la carte sans contact et le lecteur est souvent supérieure à la distance nominale de fonctionnement; le (vrai) lecteur est pourtant convaincu que le (vrai) tag est dans son champ RF.



Attaques RF

- **Attaque « man in the middle »:** même principe que l'attaque Relais mais lors du passage des informations dans le relais , le but est de modifier les données :

  - Décrypter
  - Modifier
  - Ré-encrypter

Attaques RF

- **Brouillage :** l'objectif est de brouiller le signal du lecteur en émettant un rayonnement suffisamment important (supérieur aux limites de la norme) sur la même bande de fréquence que le lecteur et avec une bande passante au moins égale.

- **Side channel :** Cette attaque consiste à espionner l'activité interne de la puce afin d'y déceler des secrets (clé secrète, algorithme de cryptage) . Seule l'attaque RFA est spécifique au lien RF**.**

  RFA (RadioFrequency Analysis) : Enregistrement du rayonnement électromagnétique émis (en dehors des communications) par un tag au travers de son antenne.

Attaques RF

- **Exposition à un rayonnement EM très important :** le but est de détruire la puce du tag en lui soumettant des tensions supérieures aux limites acceptables**.**

- **Mauvaise utilisation de la commande Kill :**

  Un lecteur espion réussit une commande Kill →Le tag est détruit . Obtention du mot de passe par une simple requête du lecteur au tag (s'il n'est pas protégé).

Contremesures

- **Le brouillage actif :** on protège les tags que l'on détient d'un éventuel lecteur espion en émettant un champ EM afin de le brouiller son signal . Ce procédé est illégal car il peut endommager les systèmes sans contact à proximité si le champ est de forte puissance → déni de service

- **Distance Bounding :** Algorithme qui définit un temps maximum de réponse du tag aux requêtes du lecteur. Si celui si est trop long , il stoppe la communication en suspectant une attaque relai.

Contremesures

- **Utilisation d'une cage de Faraday :** On place le tag dans une cage de Faraday qui ne laisse pas passer les ondes électromagnétiques afin de le protéger de toute attaque de type skimming.

- **Interrupteur :** On place une interrupteur entre la puce et l'antenne. Le problème est de savoir dans quelle position se trouve l'interrupteur…

Contremesures

- **Bruit pseudo aléatoire:** échange confidentiel de clés.

1. Le tag bruyant émet une bruit numérique N(i) par une séquence de bits pseudo-aléatoire
2. Au même moment, le lecteur envoie les bits de la clé sécurité k(i)
3. Un espion voit N(i) + k(i) (incompréhensible)
4. Le tag soustrayant N(i) retrouve k(i)

Contremesures

- **Les protocoles bloquants:**
  - **RFID guardian** : permet le blocage des lecteurs non autorisés en vérifiant la validité des requêtes reçues.
  - **Blocker Tag** : simule et envoie plusieurs possibilités d'UID au lecteur → création de collisions

    Problème : tous les tags sont ensuite bloqués par le temps de gestion des collisions → déni de service

Contremesures

- **Limitation de la distance de fonctionnement :** afin d'éviter toute écoute de la conversation entre le lecteur et le transpondeur par un espion, on limite la distance de fonctionnement du système. L'espion devra donc se trouver très proche de sa victime.

- **L'usage de la cryptographie :** les données sont cryptées grâce à une ou plusieurs clés connues du lecteur et du transpondeur. L'espion ne pourra comprendre la conversation que s'il parvient à décrypter les données.

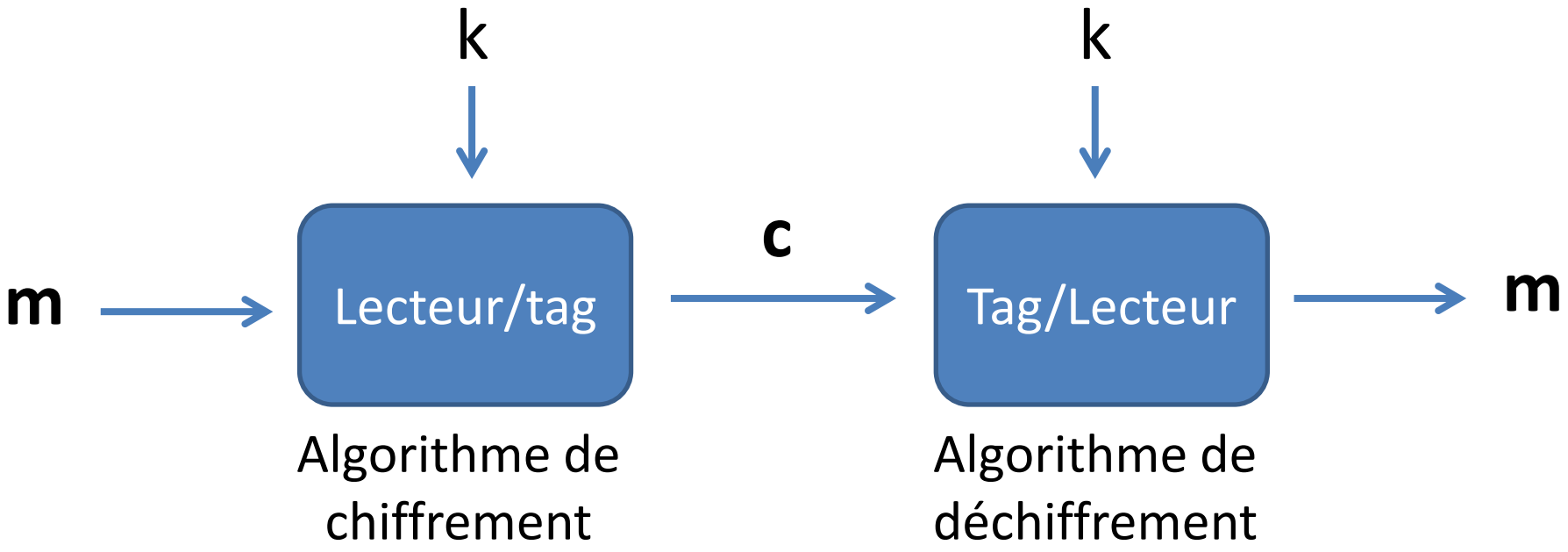
Cryptographie

- **La cryptographie symétrique**
  - DES, AES, …
  - Ne repose que sur une seul clé (privée).
  - Problème : gestion des clés

- **La cryptographie asymétrique (ie clé publique).**
  - RSA, ECC, …
  - Repose sur deux clés (clé publique et clé privée).
  - Microprocesseur requis pour le tag.
  - Travail en cours afin de réaliser une PSK (Public Key Cryptography) sans microprocesseur (algorithme GPS, Orange)

Cryptographie

- **La cryptographie symétrique**
  - **La clé de chiffrement est la même que la clé de déchiffrement**



Cryptographie

- **La cryptographie symétrique**
  - **DES** (Data Encryption Standard)
  - **AES** (Advanced Encryption Standard) : destiné à remplacer le DES.
    - standard, sans restrictions d'usage , ni brevet (comme DES)
    - algorithme de chiffrement par blocs (comme DES)
    - supporte différentes combinaisons [longueur de clé] [longueur de bloc] : 128-128 ; 192-128 ; 256-128 .

En conclusion, AES répond aux mêmes exigences que DES mais il est beaucoup plus sur et flexible .

Cryptographie

- **La cryptographie symétrique**

Avantages
 - Système rapides (implantation matérielle) - Clé relativement courtes (128 ou 256 bits)

Inconvénients
 - Gestion des clés difficiles (nombreuses clés) - Point faible = échange d'un secret

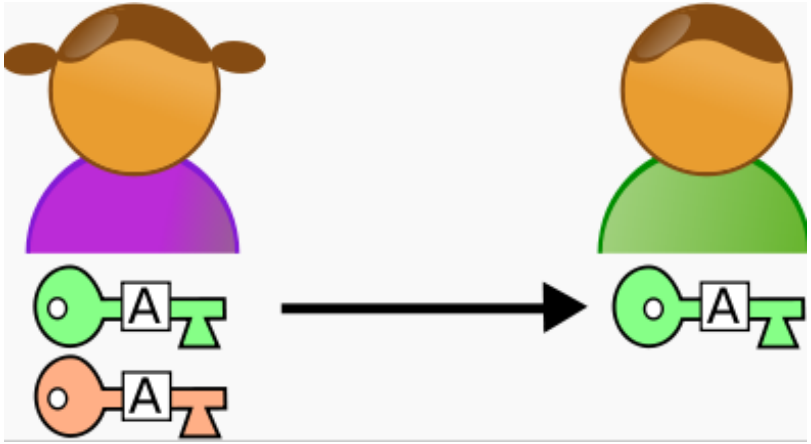
Cryptographie

- **La cryptographie asymétrique**

La clé de chiffrement (pk) est publique sert à chiffrer les données.

La clé (sk) reste privée et sert au déchiffrement uniquement.

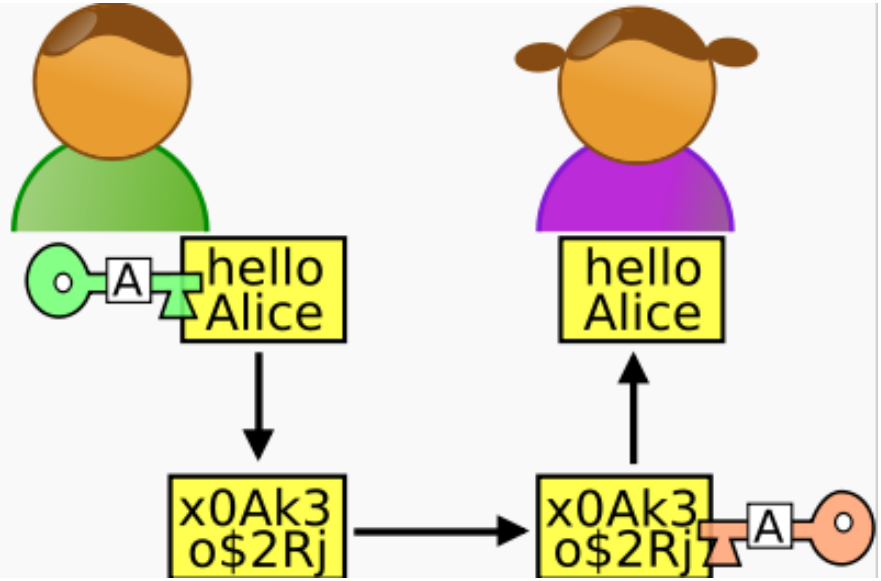
Exemple : Alice et Bob veulent communiquer de façon sécurisée .



1ere étape : Alice génère deux clefs et communique la clef publique tout en en gardant secrète la clef privée.

Cryptographie

- **La cryptographie asymétrique**

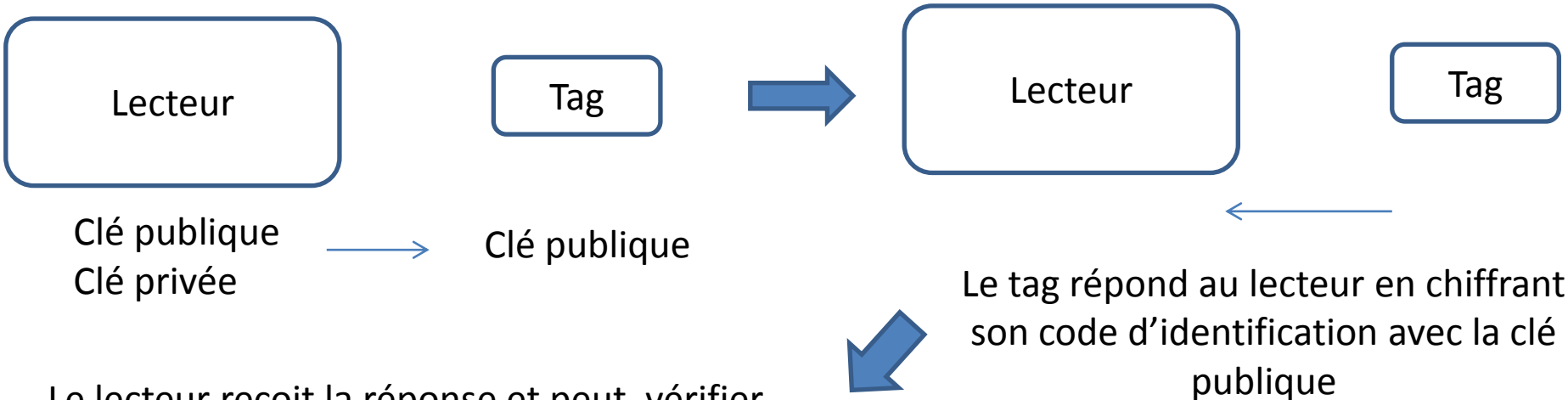


2éme et 3éme étape :
Bob chiffre son message avec la clef publique et envoie son message chiffré à Alice.
Alice déchiffre le message de Bob grâce à la clé privée.

Cryptographie

- **La cryptographie asymétrique**

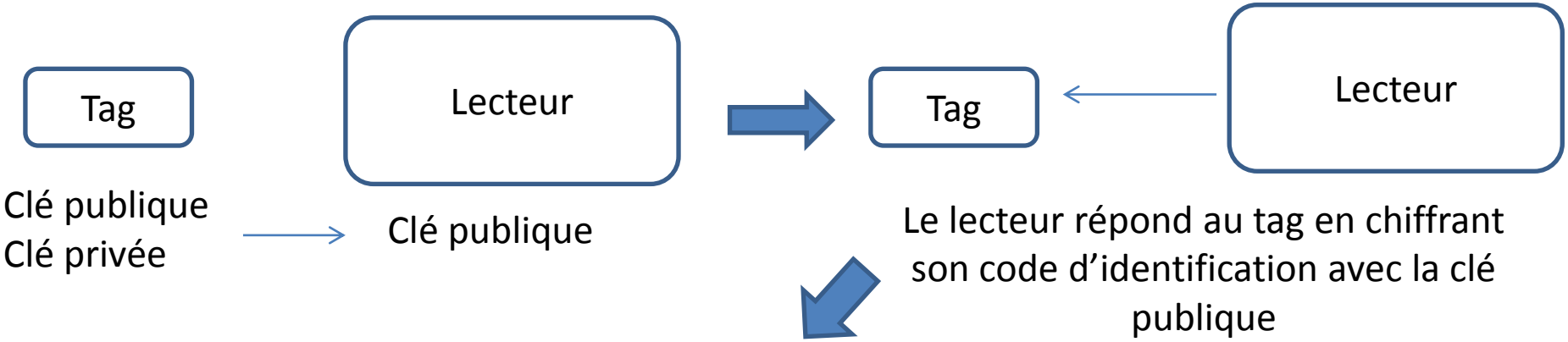
Authenticité du tag :



Cryptographie

- **La cryptographie asymétrique**

Authenticité du lecteur :



Le tag doit donc maintenant déchiffrer la réponse du lecteur avec sa clé privée pour identifier le lecteur → Peut poser problème car cela exige une puissance de calcul et une consommation d'énergie importante (difficile pour un tag UHF passif)

Cryptographie

- **La cryptographie asymétrique**

  - **R.S.A** (Rivest, Shamir, Adleman) : est le système cryptographique à clé publique le plus utilisé nos jours. Il repose sur trois algorithmes :
    - Algorithme de génération de clé
    - Algorithme de chiffrement
    - Algorithme de déchiffrement
  - **E.C.C** (Elliptic Curve Cryptography) : L'usage des courbes elliptiques permet :
    - D'utiliser des clés plus courtes qu'avec un système RSA.
    - Un niveau de sécurité équivalent ou supérieur aux autres méthodes.

    En revanche, cette méthode peut s'avérer plus complexe sur les opérations de chiffrement et de déchiffrement.

    De plus, elle n'est pas très connue car elle souffre d'un très grand nombre de brevets ,ce qui empêche son développement.

Cryptographie

- **La cryptographie asymétrique**

Bilan:

Avantages
 - Gestion des clés plus faciles - Aucun transfert de clef privée (confidentialité)

Inconvénients
 - Complexe - Système 100 à 1000 plus lent que le symétrique

Sommaire

- Le Centre National de référence RFID
- RFID : un mot, plusieurs technologies… les classifications possibles
- Identification automatique : quand la RFID s'impose…
- Etat de l'art des performances RFID : à quels prix
- Marchés et applications phare
- Focus sur l'encodage
- Aspects sécuritaires
- Tour d'horizon des aspects réglementaires, sanitaires et sociaux
- Conclusion

Normalisation

- Quelques mots de vocabulaire
- La régulation
- Les réglementations
    - Exposition aux ondes EM
    - Respect de la vie privée
    - Sécurité
    - Logos et signes
- Les normes techniques
- Conclusion

Normalisation

Une **réglementation** (ou *règlementation*) est un ensemble d'indications, de lois, de prescriptions, de règles, régissant une activité sociale.
Les règlementations sont rédigées par les administrations compétentes.

Une **régulation** cherche à donner une certaine stabilité à un système. La régulation peut se faire à travers des règlements.

Normalisation

Une **Norme** (définition ISO) est un « Document établi par **consensus** et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats garantissant un niveau d'ordre optimal dans un contexte donné. »

Dans certains cas, le droit peut imposer l'utilisation d'une norme.

Normalisation

Un **standard** est un référentiel n'ayant pas obligatoirement fait l'objet d'un examen collectif et d'une recherche de consensus technique, comme c'est le cas d'une norme (exemple : format de fichier pdf)

En anglais, il n'y a pas de différence entre norme et standard (norme se traduit par *standard*). On peut faire la distinction entre *standard de jure* (According to law; by right) et *standard de facto* (de fait)

Normalisation

Une **recommandation** est, en droit international, un texte dépourvu, en principe, de force obligatoire pour les Etats parties, qui fournit seulement des mesures à prendre.

Une **directive** est un acte normatif pris par les institutions de l'**Union Européenne** et intégré dans le droit de chaque pays membre. Une directive donne des objectifs à atteindre par les pays membres, avec un délai. Ce délai permet aux gouvernements nationaux de s'adapter à la nouvelle réglementation

Un **règlement communautaire**, contrairement à une directive, s'applique totalement et directement sans aucun délai.

Régulation

Définit :

- les bandes de fréquence allouées à la RFID (et tout autre système RF)
- les puissances (UHF) et champs (HF) maximum autorisés
- le taux d'occupation de la bande spectrale

Assure la coexistence entre les différents utilisateurs des ondes radio (notamment les SRD-NS).

Régulation

UIT

(Union Internationale des télécommunications)

MOU

CEPT/ERC

Conférence Européenne des administrations des Postes et Télécommunications/Comité Européen des Radiocommunications

ETSI

(European Technical Standard Institute)

ARCEP

Autorité Régulation Communications Electroniques et des Postes

ANFr

Agence Nationale des Fréquences

Régulation

CEPT/ERC RECOMMENDATION 70.03: Short Range Devices

EN 300 220 : (ETSI/ERM), Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW.

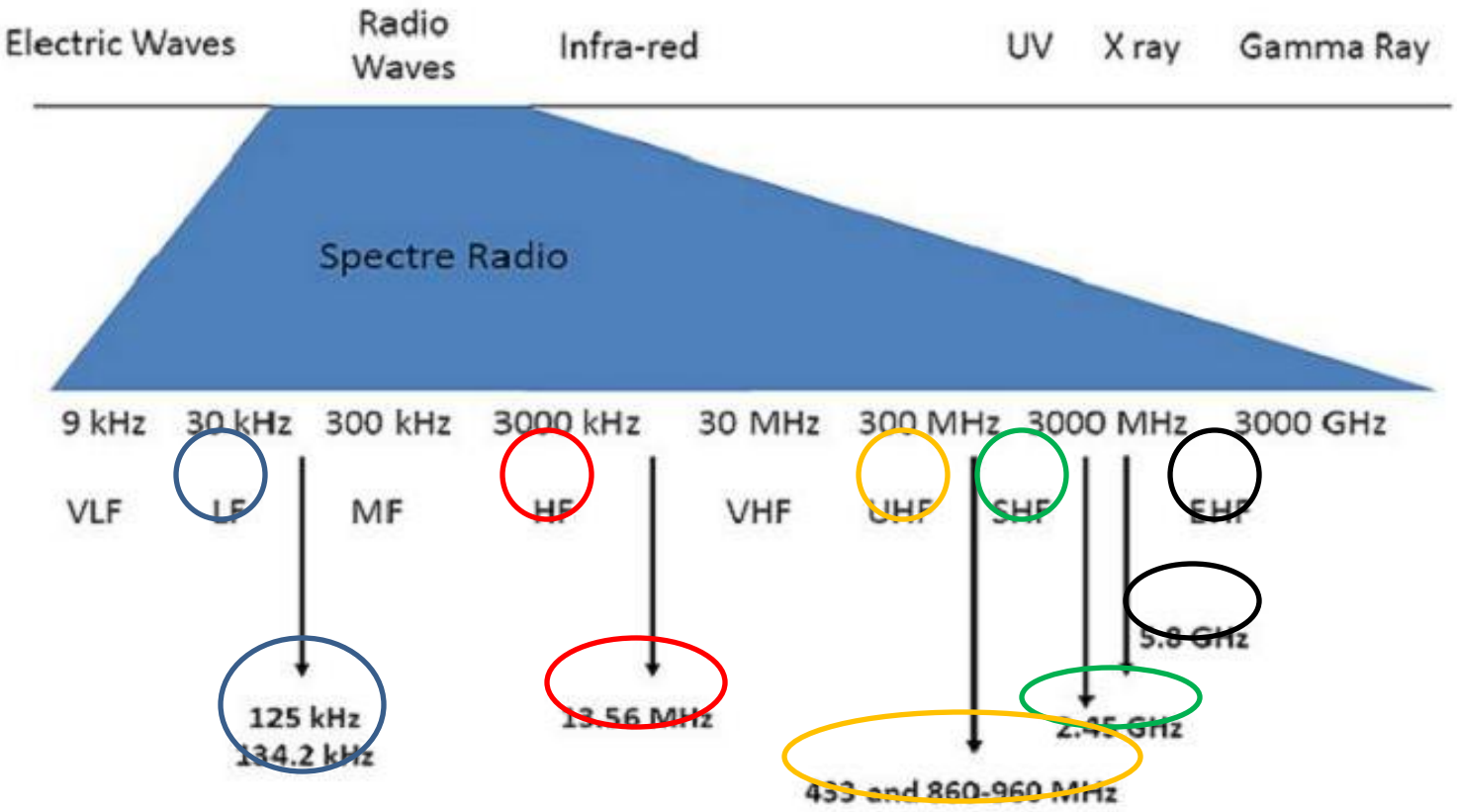
EN 300 330 : (ETSI/ERM), Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz.

EN 300 440 : (ETSI/ERM), Short range devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range.

Directive 1999/05/EC (Europe R&TTE) (Radio & Telecommunication Terminal Equipment)

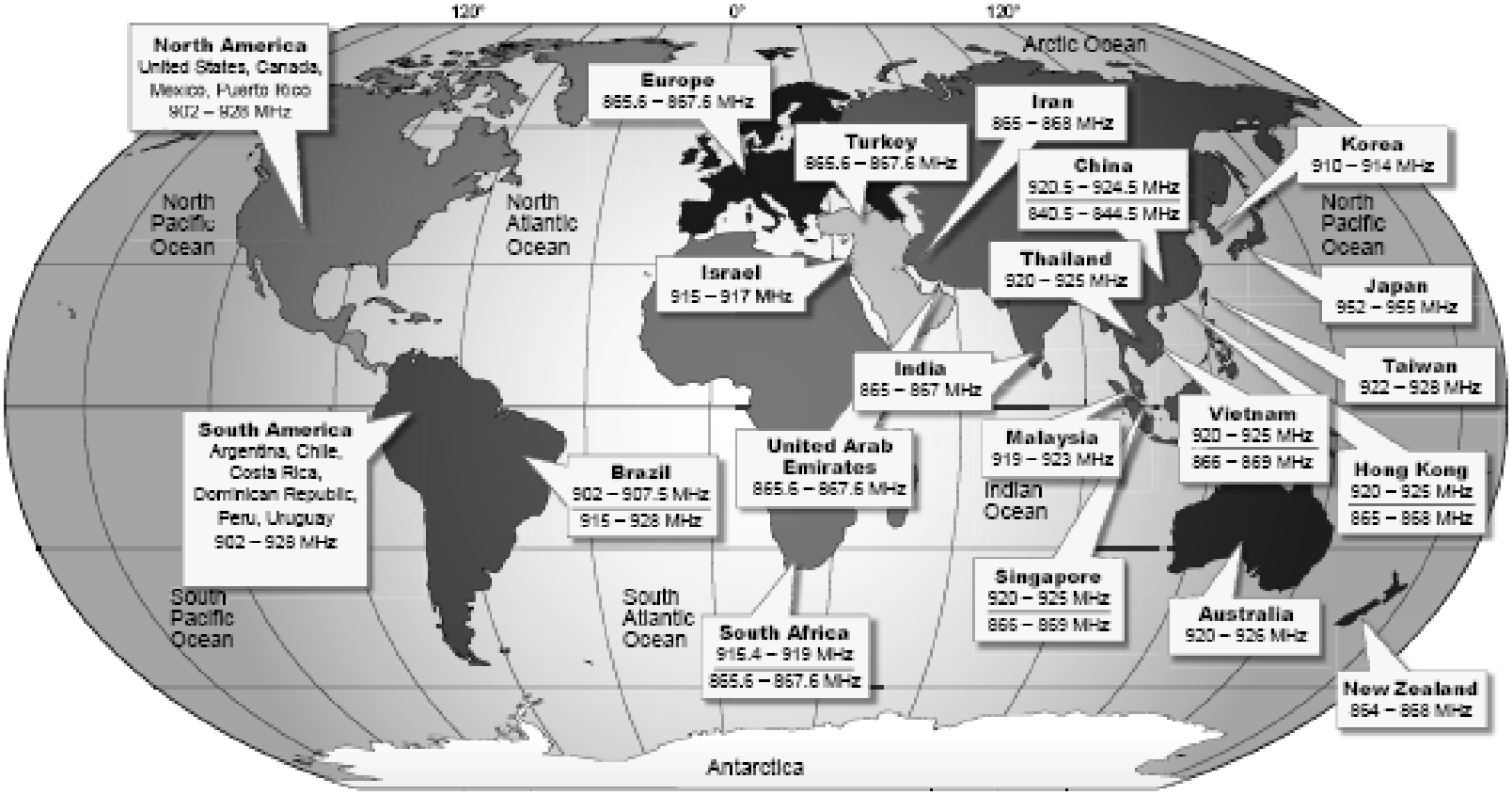
Régulation

- **Caractérisation des systèmes en fonction de leur fréquences de fonctionnement :**



Régulation

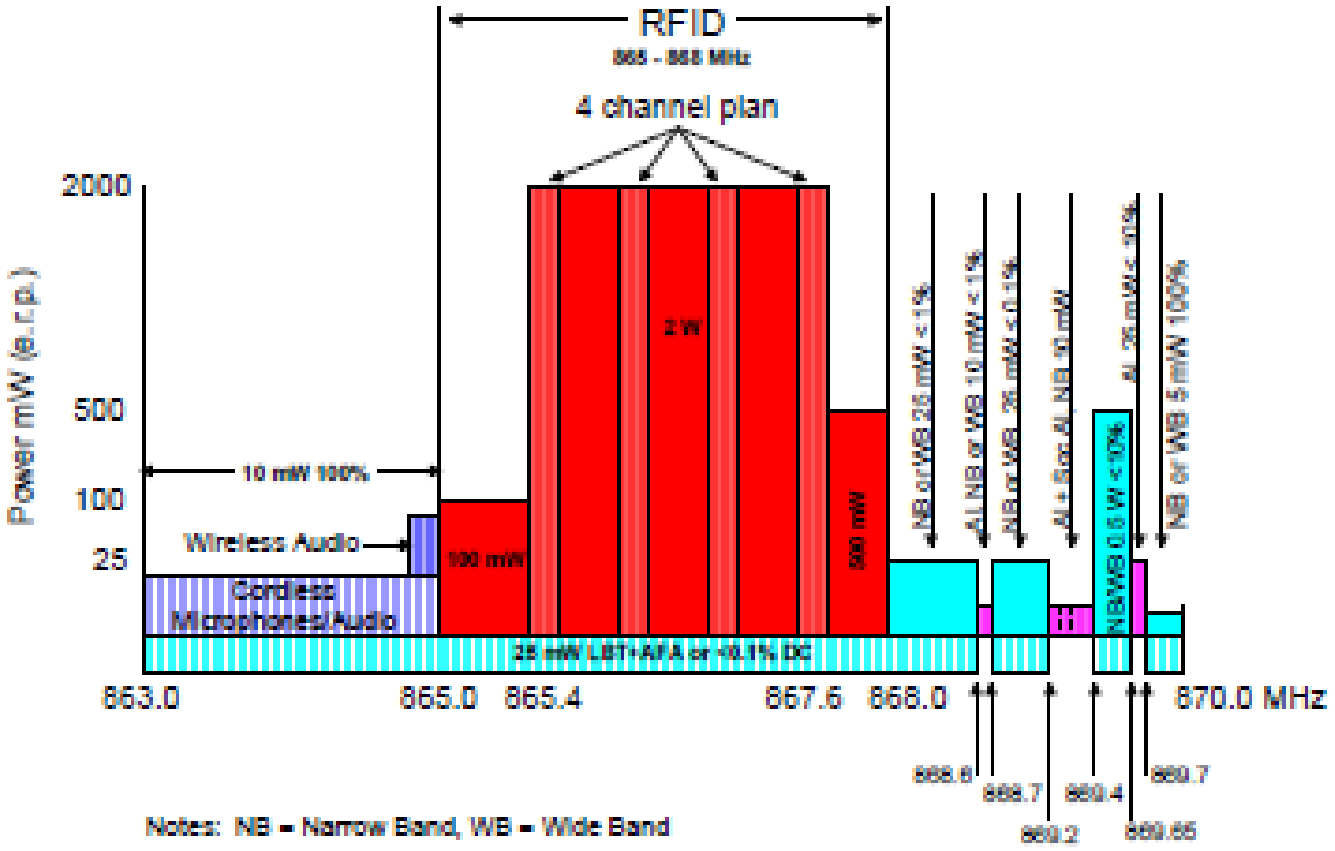
Worldwide RFID UHF Map*



*Data based on GS1 EPCglobal report dated 5 Jan 2009. Accuracy not guaranteed. Subject to change.

Régulation

SPECTRE UHF



Notes: NB = Narrow Band, WB = Wide Band

Band 869.2 - 869.4 sub-divided as follows:-

869.2 - 869.25 Social alarms < 0.1%

869.25 - 869.3 Alarms <0.1%

869.3 - 869.4 Alarms < 1%

Exposition humaine

Les organismes concernés et délivrables :

ICNIRP : International Commission on Non Ionizing Radiation Protection

Guideline for limiting exposure to time varying electric, magnetic and electromagnetic fields (up to 300 GHz)

IEEE : Institute of Electrical & Electronic Engineers

494-522 Guidelines for Human exposure

IEC : International Electrotechnical Commission

62369-1 Evaluation of Human exposure to EM of SRD used in EAS RFID and alike (0-300GHz)

CENELEC Centre Européen pour la Normalisation en Electrotechnique
EN 50357:2001 human exposure to electromagnetic fields from devices used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications

Exposition humaine

On définit:

- Un niveau maximum d'exposition (Maximum Permissible Exposure) et un taux d'absorption (Specific Absorption Rate)
- Deux types de population (professionnels et grand public)

Pour les applications RFID :

$SAR = (\sigma \mid E \mid^2)/\rho = c\,\Delta T/\Delta t$ mW / g

avec :

σ = conductivité des tissus humains S/cm

ρ = densité des tissus humains g/cm3

c = capacité calorifique des tissus humains Joule/g/°C

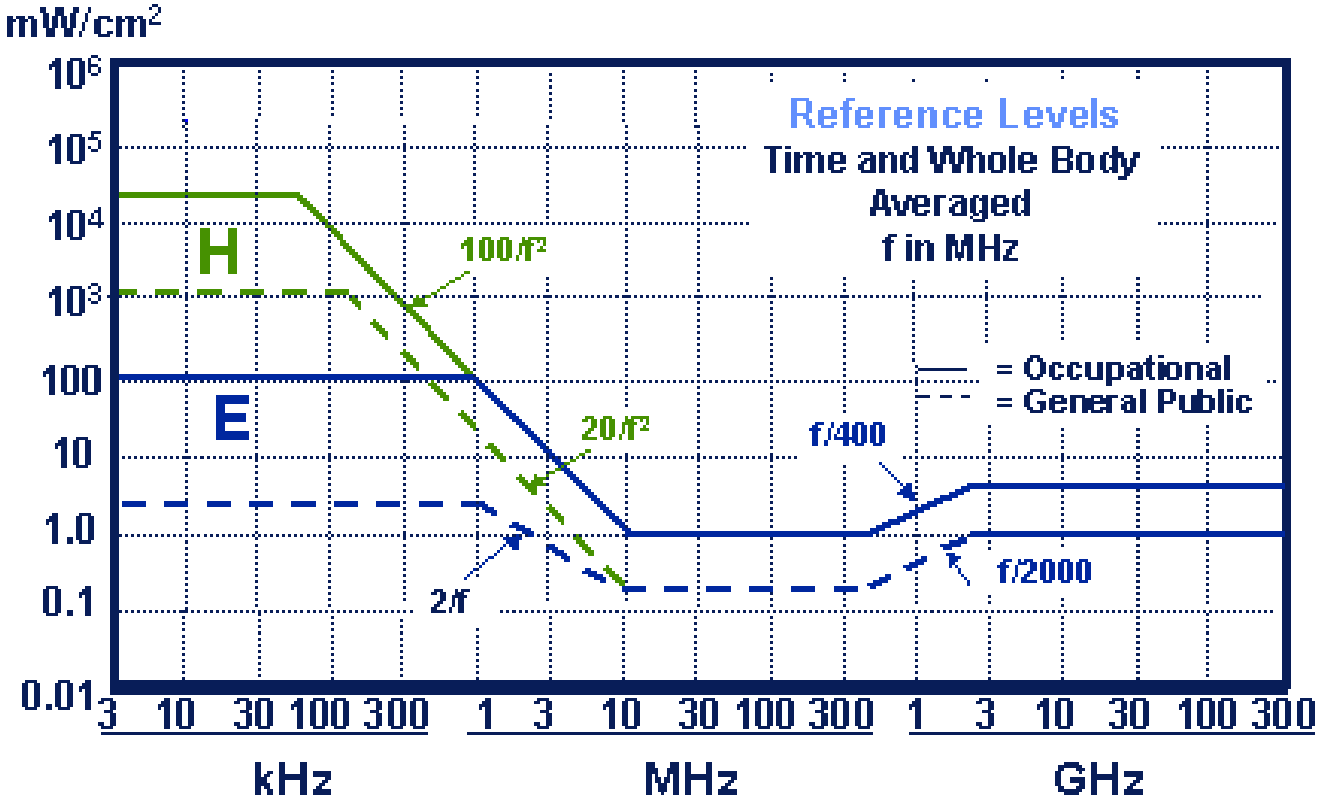
E = champ électrique V/cm

ΔT = écart de température °C,

Pendant le temps Δt, s

Exposition humaine

International Council on Non-Ionizing Radiation Protection (ICNIRP)



Exposition humaine

Le CNRFID en collaboration avec GS1, Renault et l'AFNOR a publié une procédure simplifiée d'évaluation des niveaux d'exposition

Document libre de droit téléchargeable depuis le site www.centrenational-rfid.com

Pour une conformité "officielle", il faut suivre la norme EN 50357 avec des mesures en laboratoire.

Les travaux en cours concerne les interférences possibles avec les implants médicaux…

Privacy

Les acteurs concernés :

CNIL : Commission Nationale Informatique et liberté

EC : *Directive 2002/58/EC: Processing of personal data and protection of privacy*

Mandat 436 publié en 2009

Recommandation 12 mai 2009

Associations de consommateurs

Grand public

Privacy

- **Retour en 2003**
  - Décision de Wal-Mart d'imposer la RFID à ses fournisseurs
  - Déploiements massifs potentiels
  - Jusqu'au consommateur
- **Médiatisation de la RFID**
  - Auprès du grand public
  - Auprès des entreprises
  - Auprès des décideurs
  - Canal Internet destructeur pour l'image de marque de la RFID
- **Préoccupations exprimées**
  - Captation d'informations personnelles via la RFID
  - Intelligence économique (entreprises, Etats)
  - Enjeux de souveraineté pour les Etats

Privacy

Recommandation européenne de mai 2009

« mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur la RFID »

- **Titre**
  - **« Protection des données » : pas <u>que</u> données personnelles**
- **Définitions & Périmètre**
  - **RFID au sens large, y compris la NFC**
  - **Tous secteurs d'activité, sauf… applications gouvernementales**
  - **Focus sur la distribution (lien au consommateur-citoyen)**

Privacy

- **Tout est centré sur la désactivation du Tag**
- **Logique**
  - **Désactivation définitive sécurisée (Kill + passwords)**
  - **Désactivation définitive non sécurisée (Kill)**
- **Physique**
  - **Destruction physique (languette, électromagnétique,…)**
  - **Désolidarisation du tag au produit**

Privacy

- **La recommandation « oblige » à la désactivation mais subordonne ses conditions d'exécution aux conclusions d'un PIA (Privacy Impact Assessment)**

  - **Désactivation systématique (OPT-IN) à la charge du distributeur dans le cas où l'application présente un risque probable pour la vie privée ou la protection des données à caractère personnel.**

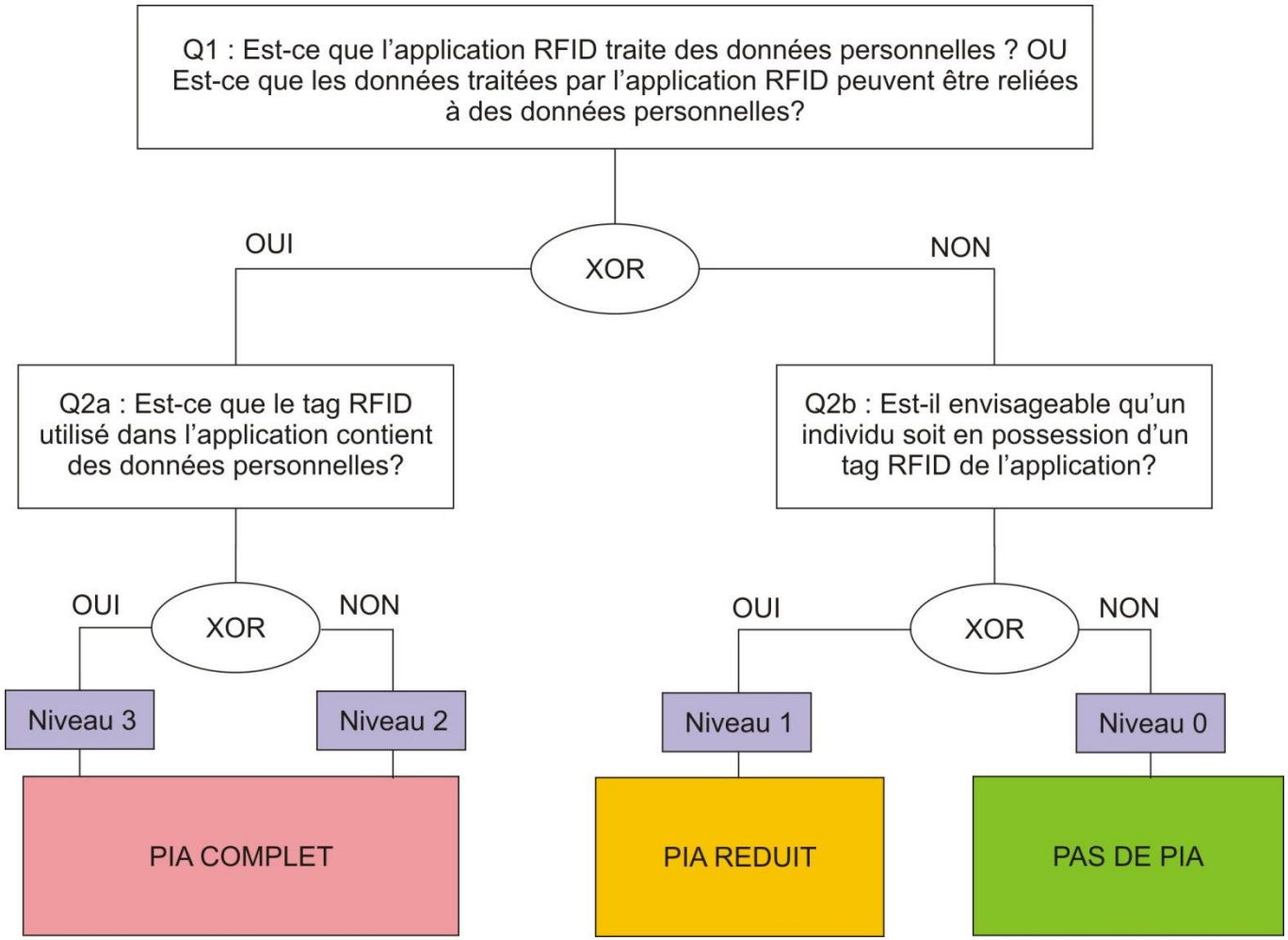
  - **Mettre à disposition un moyen simple , immédiat et gratuit de désactivation à la demande (OPT-OUT)**

Privacy

- **Evaluation d'impact (PIA)**
  - **Identifier les incidences de la mise en œuvre de l'application / données personnelles et vie privée**
  - **A conduire par chaque exploitant**
  - **Niveau de détail cohérent avec niveau risque**

- **Actions**
  - **Mesures techniques et/ou organisationnelles**
  - **Référent « données personnelles »**
  - **Mise à disposition de l'évaluation au moins 6 semaines avant déploiement**

Privacy


Q1 : Est-ce que l'application RFID traite des données personnelles ? OU Est-ce que les données traitées par l'application RFID peuvent être reliées à des données personnelles?
OUI
XOR
NON
Q2a : Est-ce que le tag RFID utilisé dans l'application contient des données personnelles?
Q2b : Est-il envisageable qu'un individu soit en possession d'un tag RFID de l'application?
OUI
XOR
NON
OUI
XOR
NON
Niveau 3
Niveau 2
Niveau 1
Niveau 0
PIA COMPLET
PIA REDUIT
PAS DE PIA

Privacy

- Carte de fidélité
  - contient un n° unique personnel => niveau 3
- Gestion des ouvrages d'une bibliothèque
  - données reliées à des informations personnelles mais pas de données personnelles dans le tag => niveau 2
- Emballages de produits consommables
  - RFID utilisée pour des besoins logistiques
  - emballage jeté/recyclé par le consommateur
  - un individu peut posséder un tag RFID de cette application à un moment donné => niveau 1
- Maintenance industrielle
  - suivi des essieux de train, de servocommandes aéronautiques, …
  - pas de données personnelles dans l'application, peu de chance qu'un individu soit en possession de ce type de tag => niveau 0

Privacy

- **Quid des applications déjà déployées et opérationnelles ?**
  - **Recommandation rétroactive ?**
  - **Evaluation d'impact, marquage, information**
  - **Télépéage, clés de voiture, contrôle d'accès, etc.**
- **Quid des technologies non RFID pures ?**
  - **Incluses par défaut dans la reco : NFC, sans-contact**
  - **Exemple du téléphone mobile : double marquage, politique d'information, etc.**
- **Quels moyens de vérification si déploiement massif de la RFID ?**
  - **Etablissement des certificats**
  - **Contrôles**
- **Les questionnements de l'UE doivent servir d'exemple partout dans le monde…**

Signalisation

ISO/IEC : Norme **29160** : RFID Emblem

CEN/TC225 : prEN **16570**: signage

RFID tags may be read in this area for the purpose of stock control security and product warranty

This system is controlled by French RFID National Centre (CNRFID)

For more information contact us on:
+33 494 370 937
or visit our website
www.centrenational-rfid.com

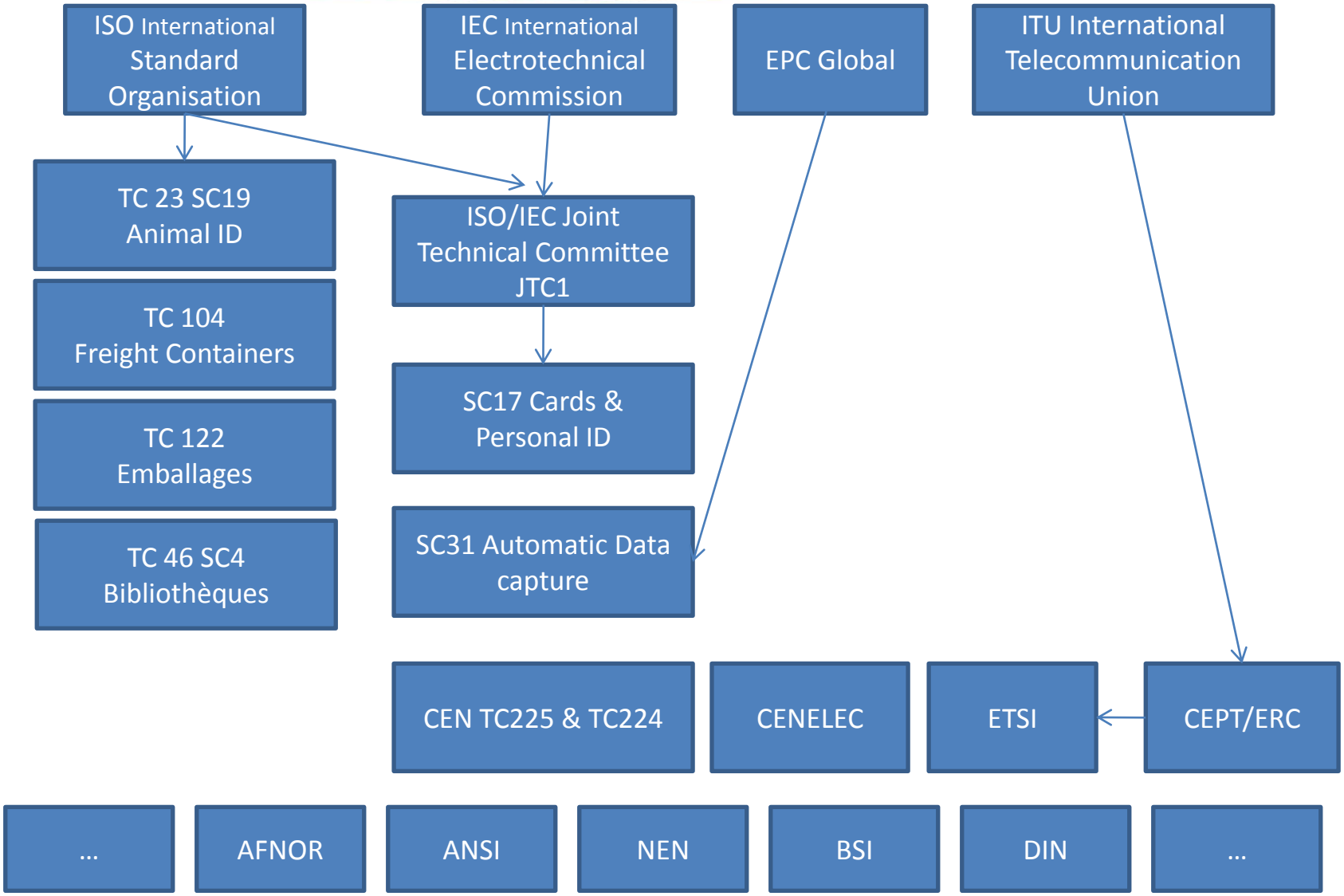
Signalisation

- **Jusqu'où va la signalisation ?**
  - **Sur chaque produit portant une étiquette RFID ?**
  - **Pour signaler la présence d'interrogateurs ?**
  - **Pour signaler la présence d'antennes ?**
  - **etc.**

- **Que doivent indiquer les logos ?**
  - **La présence de RFID (NFC inclus ? Et le zigbee ?)**
  - **Le type de fréquence utilisée ?**
  - **Pourquoi pas le protocole (EPC vs. 18000-6 D, etc.)**

- **Utile si le grand public peut interagir avec les étiquettes**

Normes techniques



Normes techniques

Les Working Groups ISO/IEC JTC1 SC31: (Automatic Identification and Data Capture)

- **WG1**: Symbology
- **WG2**: Data Structure
- **WG3**: Conformance
- **WG4**: Air Interface
- **WG5**: Real Time Locating Systems (RTLS)
- **WG6**: Mobile Identification and Item Management (MIIM)
- **WG7**: Security and File Management

Normes techniques

WG4/SG3 : Air Interface

18000-1 : Définition des paramètres à normer

18000-2 : Air interface communication below 135kHz *(2 modes: 125 KHz, 135 KHz)*

18000-3 : Air interface communication @ 13.56 MHz *(3 modes)*

18000-4 : Air interface communication @ 2.45 GHz

18000-6X : Air interface communication @ 860-960MHz (4 modes: Mode A, mode B, mode C (# EPC), et D (Total))

18000-7 : Air interface communication @ 433 MHz

Normes techniques

WG4/SG6: Conformance & Performance

18047-2:	135 KHz
18047-3:	13.56 MHz
18047-4:	2.45 GHz
18047-6:	860-960 MHz
18047-7:	433 MHz

Normes techniques

WG4/SG6: Conformance & Performance

18046-1: Tests performance des systèmes RFID

18046-2: Tests performance des interrogateurs

18046-3: Tests performance des tags

Normes techniques

Les normes RFID du comité SC17 (smartcards and personnal ID)

14443-X: Identification cards – Contactless integrated circuit cards – Proximity cards (4 parts), 3 modes, (10373-6 conformance)

15693-X: Identification cards – Contactless integrated circuit cards – Vincinity cards (4 parts), 3 modes, (10373-7 conformance)

Rem: équivalent à 18000-3 mode1

Interchangeabilité

- Deux produits sont interopérables s'ils arrivent à échanger des informations.
- Les tests de conformité aux normes doivent garantir l'interopérabilité.
  - Ils doivent (devraient) être fournis par les constructeurs (data sheet)
  - Ils devraient être réalisés par des laboratoires indépendants
- Un tag ISO 18000-3 mode 3 doit pouvoir communiquer avec un lecteur ISO 18000-3 mode 3
- Un tag ISO 15693 n'est pas censé pouvoir discuter avec un lecteur ISO 18000-3 mode 3

Interchangeabilité

- Pour les utilisateurs, l'interopérabilité ne suffit pas toujours…
- Les intégrateurs doivent garantir les mêmes performances.
- Si je lis un tag A à 6 mètres, je veux pouvoir lire un tag B, d'un autre fournisseur à 6 mètres !
- D'où **la nécessité** des tests d'interchangeabilité

…….Un exemple : **MASTERCARD**

Interchangeabilité

Dans la jungle des normes et des règlements, 3 attitudes sont possibles :

- Ne rien faire
  - ➢ s'exposer à des poursuites de la part du grand public (pour les utilisateurs de RFID)
  - ➢ s'exposer à des poursuites de la part des utilisateurs (pour les fournisseurs de RFID)
- Agir sur les textes
  - ➢ demande énormément de compétences et de moyens humains
- Faire confiance à un tiers neutre et indépendant

Conclusion

- **La RFID est assez mature mais doit encore relever de nombreux challenges…**

- **Son adoption repose sur sa capacité à …**
  - S'interfacer au SI existant ou à venir
  - S'adapter à des conditions d'utilisation variées (environnement, support, système d'information)
  - S'intégrer au reste des objets communicants (interopérabilité)

MERCI DE VOTRE ATTENTION

CNRFID
CENTRE NATIONAL
DE REFERENCE

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

Merci pour votre attention

www.centrenational-rfid.com

Contacts

Pour nous contacter :

CNRFID
5 avenue de Manéou
13 790 Rousset - France

- **Jean-Christophe Lecosse**, Directeur Général : 04 42 37 09 38
- **Claude Tételin**, Directeur Technique : 06 43 72 27 18
- **Marie-Noëlle Lemaire**, Responsable Projet Collaboratif : 07 85 56 04 48
- **Joffray Henné**, Responsable des Services aux Offreurs) : 06 82 36 62 84
- **Nicolas de Guillebon**, Responsable Projet NFC : 06 52 50 31 41
- **Guillaume Baelde**, Responsable des Services aux Utilisateurs : 04 75 75 98 97
- **Céline Haouji**, Responsable Communication : 04 42 37 09 41
- **Mélanie Dussere**, Chargée de communication : 04 42 37 09 37
- **Christel Poirier**, Assistante Administratif et Financier : 04 42 37 09 37
- **Florence Besnard**, Assistante : 04 75 75 98 97

Visitez nos sites web

Le site web du CNRFID

http://www.centrenational-rfid.com/

Le site web de l'International RFID Congress

http://www.rfid-congress.com/2013/