RFID Technologies: Emerging Issues, Challenges, Policy Options

A study by TNO and Telecom Italia for IPTS

TNO | Kennis voor zaken

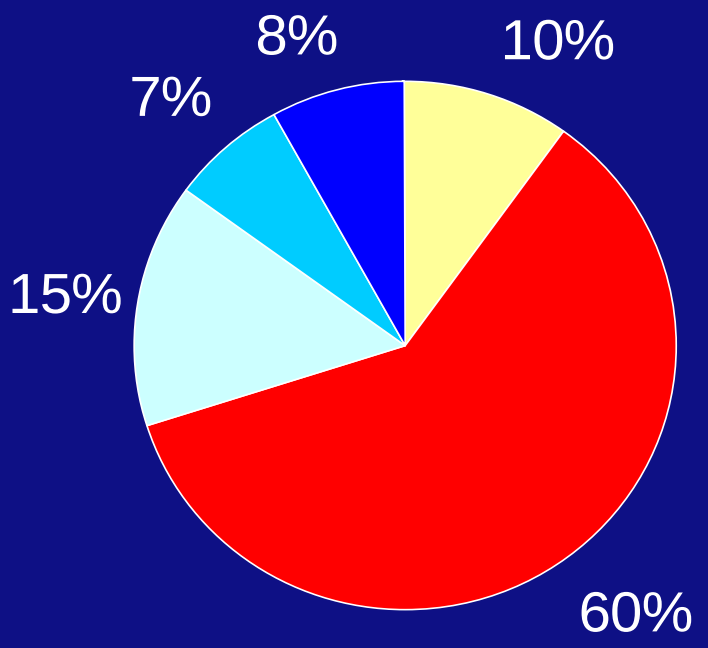
IFIP/FIDIS Summerschool Karlstad - 2007

Overview

- RFID Technologies
- RFID Markets
- RFID Privacy issues
- Conclusions

Different RFID technologies

Different RFID frequency diffusion



Passive RFIDs
Inductive Coupling (inductors):
$P(d) \alpha 1/d^3$

Range < 1 m

Range 2 - 4 m

Passive RFIDs
backscattering

Active RFIDs
RF Propagation(λ/4 Antennas)
$P(d) \alpha 1/d^2$

Range 10 - 100 m

	LF	HF	UHF	Microwave
Frequency Range	< 135 kHz	10..13.56 MHz	850..950 MHz	2.5.5.8 GHz
Read range	~10 cm	~1 m	2 ÷ 5 m	~15 m
Coupling	Magnetic, Electric	Magnetic, Electric	Electromagnetic	Electromagnetic
Application	Smart Card, Ticketing, Anti- theft, Animal tagging	Small Item Management, Anti-theft, Supply Chain	Transportation, Vehicle ID, Access/Security, Large Item Management, Supply Chain	Transportation, Vehicle ID, Access/Security, Large Item Management, Supply Chain

PROBLEM: Frequency distribution in Europe;
-not all countries 'connected'
-capacity problem in three years time

RFID Tags

Family of low-frequency tags from **Texas Instruments**

Spider 2450 Mhz tag from **RFCode**

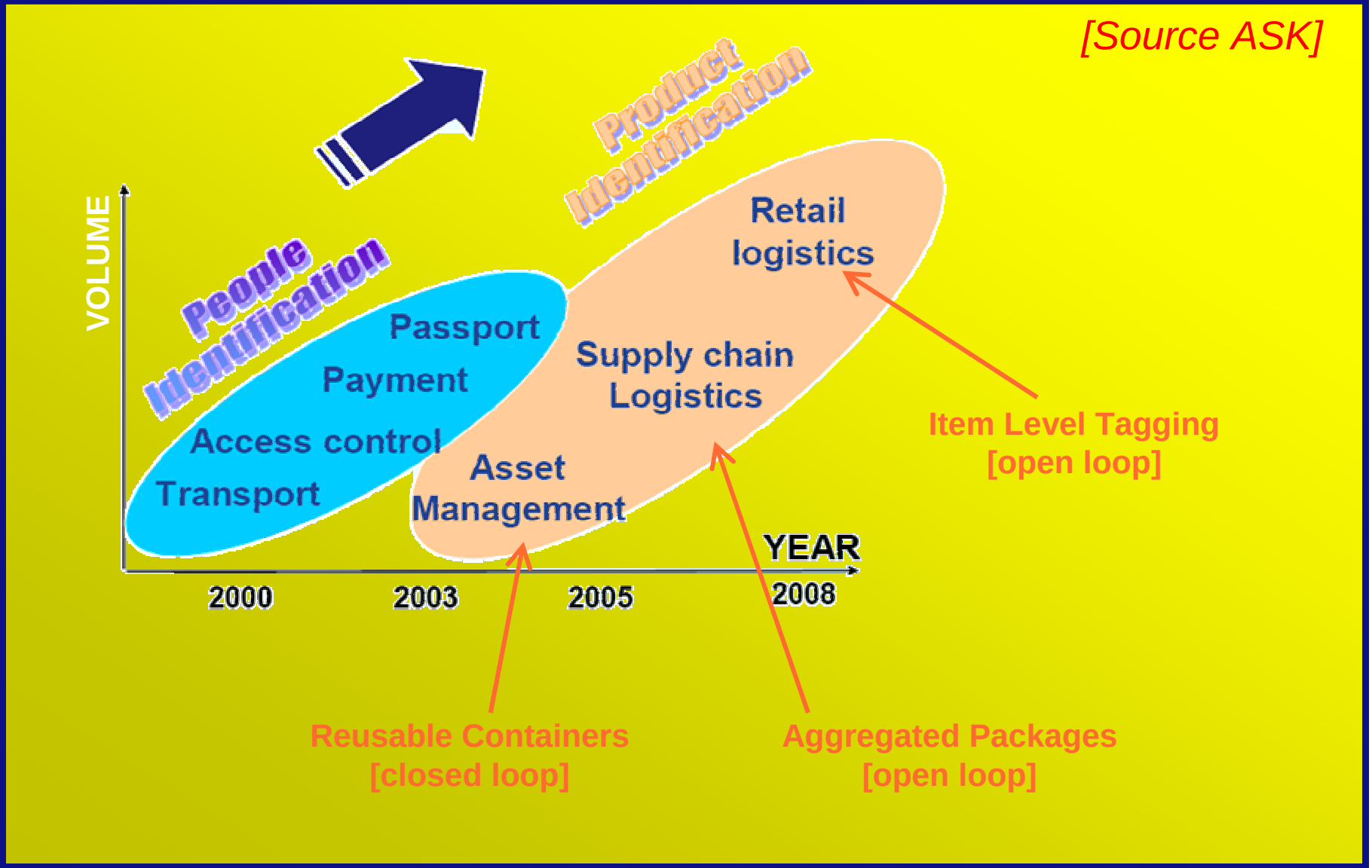
Intellitag 915 Mhz tags from **Intermec Technologies**

2450 Mhz Backscatter tag from **Alien Technologies**

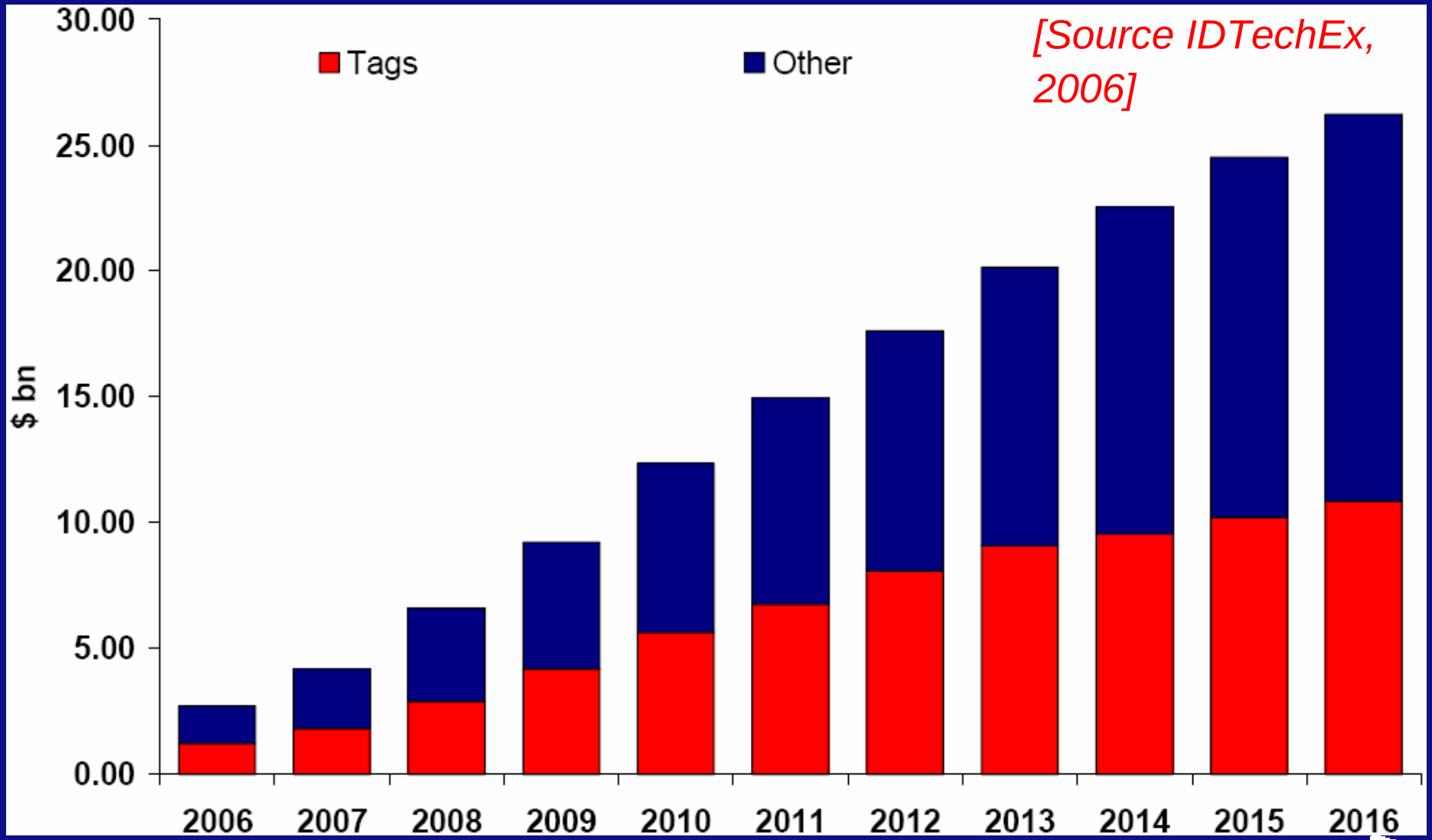
13.56 Mhz tag with largest storage capacity (4KBytes) from **Hitachi Maxell**

Smallest 13.56 Mhz EPC tags from **TagSys**

RFID applications evolution



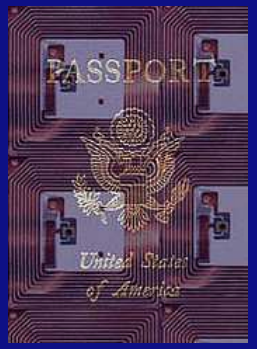
2006-2016 Market Forecast



[Source IDTechEx, 2006]

- Healthcare
  - Billion dollar market expected (2,1 B$ in 2012-2016)
  - Application domains: drug counterfeiting; error prevention (drugs, blood), locating staff, equipment, patients and visitors

- Identity cards
  - US legislation (VWP) enforces machine readable ID-cards
  - Big European market (cf. China: 6 B $; 1 B cards)

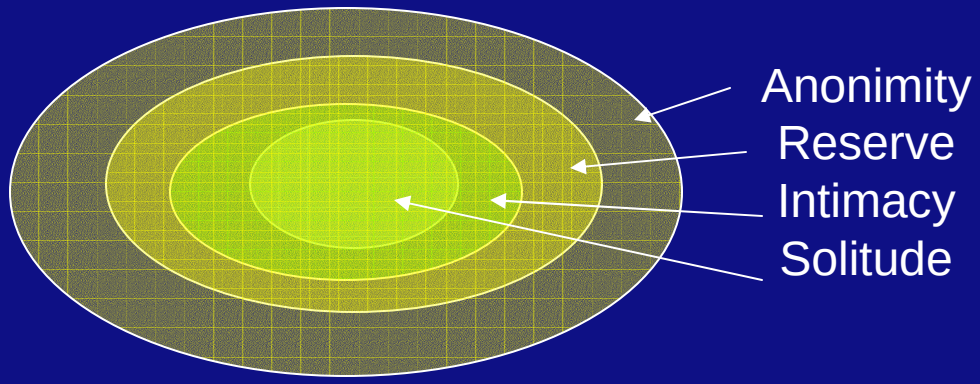


- Public transport
  - Billion dollar market (Oyster card 1.5 B Euro; Dutch PT: similar)
  - Additional services (e-purse)

- Animal tagging
  - Sheep and goats (2008); worldwide 800 M animals

Privacy issues of RFID – 1

- **Privacy**
  - **“The right to be let alone”**
  - **“The claim of individuals to decide when, how and to what extent information concerning themselves is communicated to others.” (Westin, 1967)**



- **Privacy top concern in European RFID consultation process**
  - **65% of the respondents believe that the EU should invest in technology to safeguard privacy;**
  - **60% of the respondents believe that the EU should increase awareness;**
  - **50% of the respondents believe that the EU should make specific legislation for RFID;**
  - **10% of the respondents believe that the EU should stimulate self-regulation.**

Privacy issues of RFID – 2

Consumers saying RFID has …	Greater impact	Same impact	Lesser impact	Don't know
Mobile phones	36	33	10	21
Debit cards	36	29	7	26
Credit cards	41	31	8	20
ATMs	41	32	8	19
Frequent shopper/loyalty cards	42	33	7	18
Access control badges	45	31	6	18
Smart cards	46	28	6	20
Camera phones	34	32	10	24

CapGemini, 2005

Privacy concerns related to RFID (Spiekermann, 2006)

1. Unauthorised access
2. Tracking of objects via data
3. Retrieving social networks
4. Technology paternalism
5. Making people responsible for objects.

Privacy issues of RFID – 3

Tags and sensors

Middleware ERP …

Systems Integrators

Service providers

Direct privacy concerns

Indirect privacy concerns

Privacy issues of RFID – 4

Privacy threats	Reader-tag system (direct)	Back-end (indirect)
Individual	Unauthorised reading of personal information Real-time tracking of individuals	Aggregating personal information Using data for purposes other than originally specified
Collective/ Group	-	Profiling and monitoring specific behaviour

Privacy issues of RFID – 5

- Unauthorised reading of tags
  - Eavesdropping at greater distances than indicated by suppliers (10s to 100s of meters) (Juels, 2003)
- Real-time tracking of individuals
  - Hospitals, schools, leisure parks, sport parks, imprisonment. Shopping malls?
- Aggregating (personal) data
  - Back end systems: not new but may lead to more and more intensive privacy infringements
- Using data for purposes other than originally specified
  - ‘Function creep’; E.g. data from public transport - Oyster card
- Profiling and monitoring of people
  - Back end systems

Privacy issues of RFID – 6

- **Strategies to cope with RFID privacy**
  - **Legal framework**
  - **Self-regulation**
  - **Technology ‘Privacy by design’**

Privacy issues of RFID – 7

- **Legal framework:**
  - **OECD guidelines for Fair Information Practices (1980)**
    - **Collection limitation**
    - **Data quality**
    - **Purpose specification**
    - **Use limitation**
    - **Security Safeguards**
    - **Openness**
    - **Individual participation**
    - **Accountability**
  - **EU 95/46/EC directive ('Privacy')**
  - **EU 2002/58/EC directive ('ePrivacy')**

- **Article 29 Working Party on Data Protection (2005):**
  - **Personal data**
  - **Informed consent**
  - **Electronic communication (NFC with mobile phone)**
- **European consultation process (2006): Legal measures are only limited perceived as adequate**

Privacy issues of RFID – 8

- Self-regulation
  - Centre for Democracy and Technology (USA, 2006):
  - Advantage of approach based on self-regulation:
    - Can be technology specific, can offer guidance on implementation of FIP, can be revisited and re-iterated
  - Elements of self-regulation
    - Notice
    - Choice and consent
    - Onward transfer
    - Access
    - Security

Privacy issues of RFID – 9

- Technical solutions ('privacy by design')
  - Art 29 WP (2005): "Technology may play a key role in ensuring compliance with the DP principles in the context of processing personal data collected through RFID technology."
  - OECD (2006): "The 'privacy by design approach' may be more efficient in the long run."

  - Privacy Enhancing Technologies:
    - Anonimity
    - Pseudo-identities
    - Unlinkability
    - Unobservability

Privacy issues of RFID – 10

- Solutions based on Fair Information Principles ('Scanning with a Purpose' – EPC compatible approach; Floerkemeijer, 2005)
  - Openness through reader and policy identification
  - Purpose specification in inventory command
  - Use limitation through collection types
  - Collection limitation by appropriate selection of tags
  - Watchdog tag
- Not End-of-Pipe technology but 'Life cycle' approach
- Other technical solutions:
  - Blocker tag
  - Kill tag
  - Deep sleep mode
  - Antenna destruction/removal
  - Cage of Faraday
- Problems:
  - Cost efficiency (two-way readers)
  - Encryption in low-cost RFID tags
  - Adversary consequences (guarantees, additional info on tag)

Conclusions

1. RFID is enabler of many public domain applications
2. RFID has the potential to increase the efficiency of public services (health care, public transport) and to improve the quality of life (health care, animal tracking)
3. RFID is perceived as the most intrusive technology of the past century

4. Privacy laws are problematic in dealing with RFID (Article 29 Working Party)
5. Self-regulation will not make a difference
6. There is an interesting opportunity to use technology to improve RFID-based privacy radically (Privacy by design)