

“RFID Security and Privacy ...”

ICTSB Seminar on RFID standardization
24. October 2007.

Henrik Granau

CEO RFIDsec

Member of AIM EMEA Leadership Council

Member of ATA RFID on Parts Team

Participation in EICTA's RFID Workgroup

Participation in EU's open consultation on RFID

Member of EPCglobal

- RFIDsec founded 2005
- Based upon unique Danish innovation 1999 - 2004
- Scientific Paper on RFID October 2004
- Peer Reviewed November 2004
- First Concepts launched June 2006
- First products launched September 2007



The Press' opinion



RFID Journal Editorial;

- **The most attractive security solution to hit the market so far, in my view, comes from the Danish Company RFIDsec. This solution gives control of a tag to the consumer, who would essentially have to give someone permission to read the tag for after-sales support, returns or other business applications.**



RFID Gazette;

- In the backdrop of hectic debate on the privacy concerns of RFID technology, RFIDsec's RFID tags are likely to **reduce the skepticism** of the users.



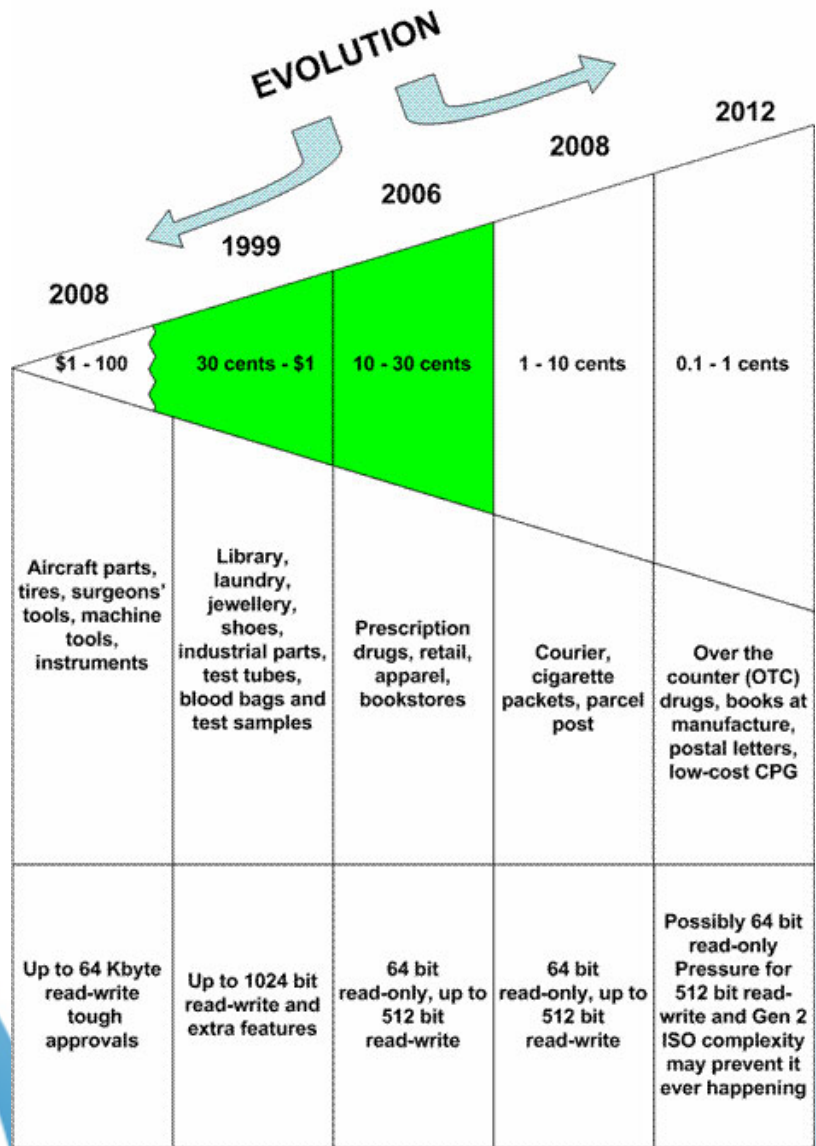
- "Embedded intelligence in things themselves will distribute processing power to the edges of the network, offering greater possibilities for data processing and increasing the resilience of the network. This will also empower things and devices at the edges of the network to take independent decisions. "Smart things" are difficult to define, but imply a certain processing power and reaction to external stimuli."



Source: ITU Internet Reports 2005: The Internet of Things

- Yesterday : "Controlled readers"
- Today : + PDA's and Mobile phones with a reader-card
- Tomorrow : + PDA's, PocketPC's and Mobile phones with embedded readers
- Future : + "Embedded readers" in anything
- And of course smaller, better, faster and cheaper ...

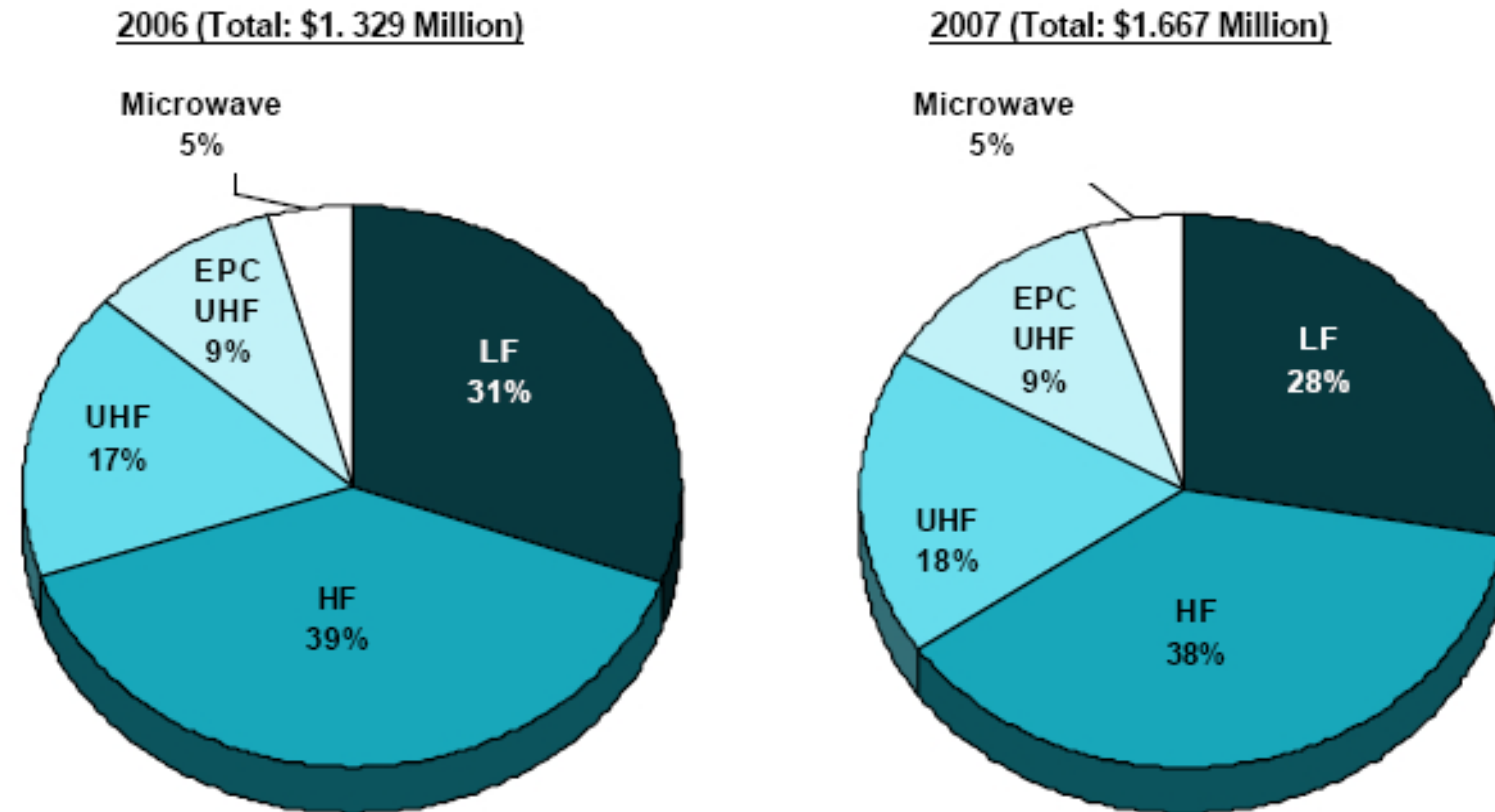
- Yesterday : "electronic barcode"
- Today : + storing data on the tags
- Tomorrow : + coupled with sensors and actuators
- Future : "Internet of Things" / Ubiquitous
- And of course smaller, better, faster and cheaper ...



APPLICATION	ULTIMATE POTENTIAL NUMBERS BILLION YEARLY	POTENTIAL BENEFITS					REMOVAL OF TEDIOUS PROCEDURES
		COST REDUCTION	INCREASED SALES	CRIME REDUCTION	BETTER SERVICE	SAFETY	
Laundry/ rented textile	0.1	•			•		•
Library books, DVDs, etc	0.1	•		•	•		•
Parts for aircraft and other machinery	1	•		•	•	•	•
Blood bags and samples	2	•			•	•	•
Military	20	•		•	•	•	•
Book manufacture	50	•	•	•	•		•
Drugs, prescription	50	•	•	•	•	•	•
Cigarettes	100	•	•	•	•	•	•
Postal	850*	•		•	•	•	•
Other Consumer Packaged Goods (CPG)	5-10,000	•	•	•	•	•	•

Source: IDTechEx

Global RFID Revenue by Frequency (Transponders & Readers Only)



Source: Venture Development Corporation

The Commission concluded from the initial analysis of public consultation results that:

- It is necessary to develop an effective set of European rules, based on transparency and choice, to support the development of RFID;
- Particular effort needs to be invested in explaining the risks and benefits of RFID to the general public;
- The issue of privacy needs to be seriously addressed, in particular through ongoing research into privacy enhancing technologies.

Commissioner Reding also highlighted the need to act on a global scale and renewed her commitment to strengthening international dialogue on RFID.

© *European Communities 2006*

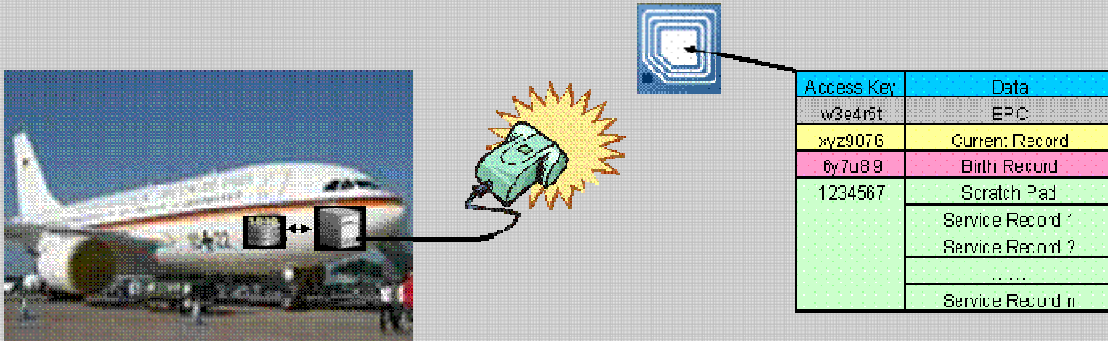
Reproduction is authorised provided the source is acknowledged.

The views expressed are not an official position of the European Commission

- The RFID tag answers anybody
- The RFID tag can easily be cloned
- Data on a RFID tag can be altered
- Communication between RFID tag and reader can be eavesdropped
- Communication between RFID tag and reader can be recorded and re-played

- RFIDsec is member of Air Transportation Association e-business program "RFID on Parts", by invitation from Boeing

■ Different data areas on the RFID can have its own Access Key(s) with associated Read and/or Write Access rights



Access Key	Data
w3e4r5t	EPC
xyz9076	Current Record
6y7u89	Birth Record
1234567	Scratch Pad
	Service Record 1
	Service Record 2

	Service Record n

■ Secure read/write data provided

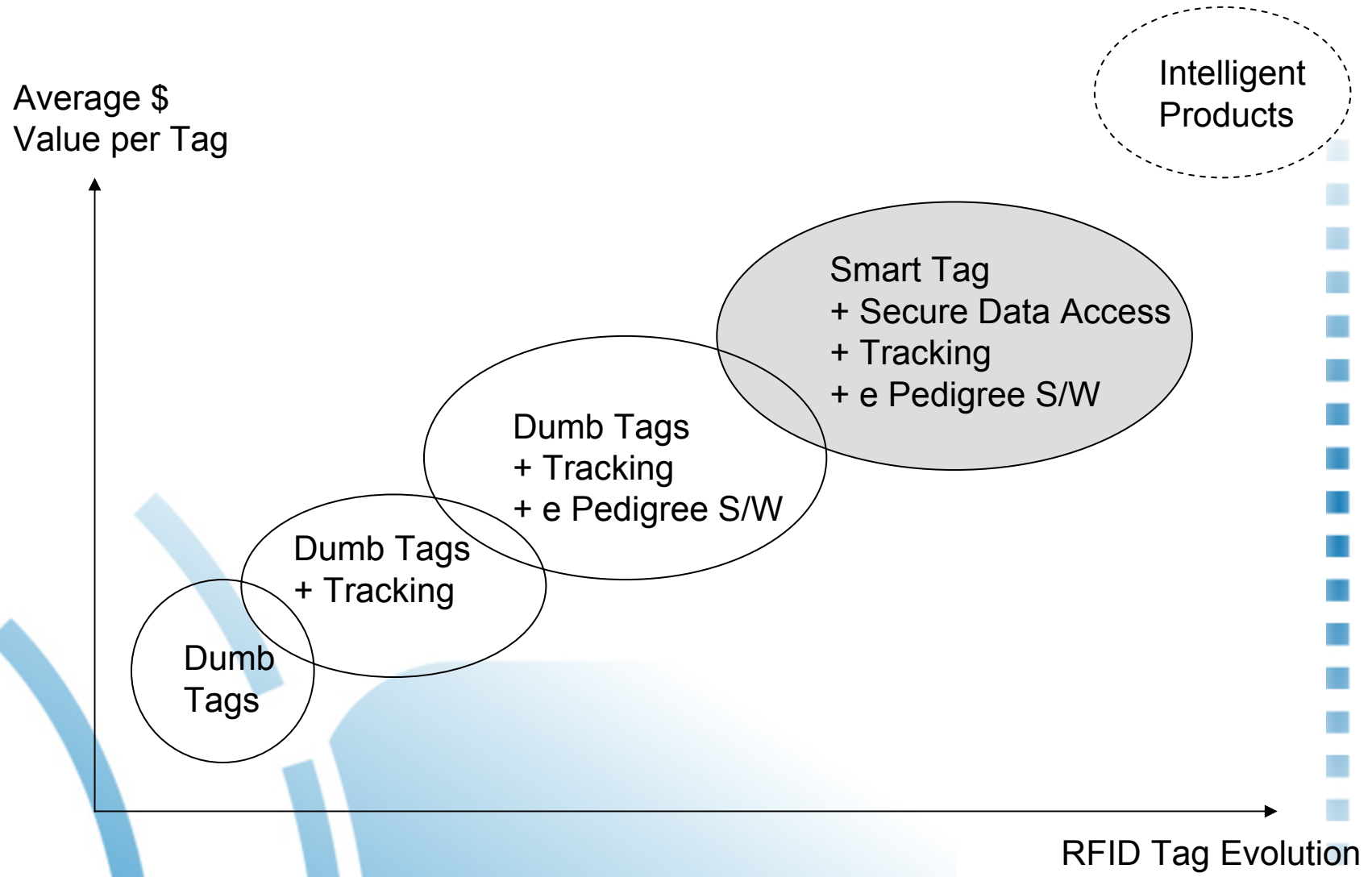
■ No unauthorised access to RFIDs

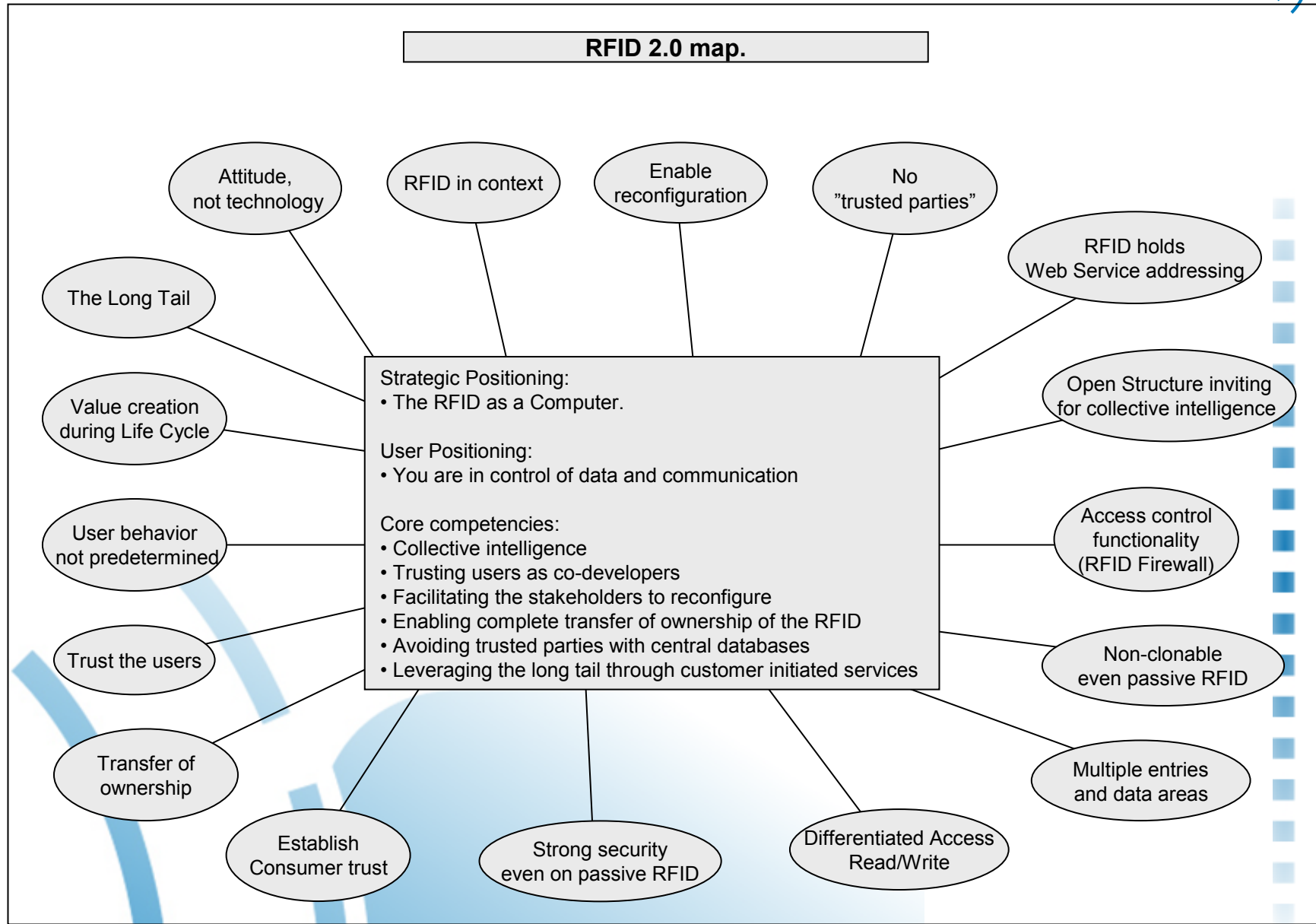
■ Part originality can be checked

■ The Service Mechanic can;

- Read and Write the Scratch Pad and the Service Records
- Read the Current Record and the Birth Record
- If specifically authorised to this, then update the Current Record

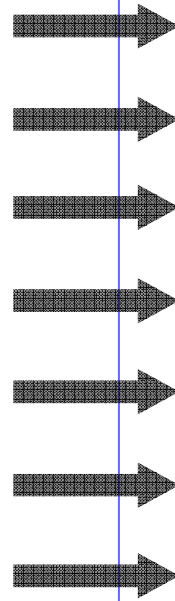
- RFID's to be used in the usual manner in Supply Chain
- RFID's to be 'deactivated' when the drug is leaving the Pharmacy
- RFID's can not be read in 'Public space'
- RFID's to be 'reactivated' when ready for consumption (Home medication, Hospitals)





RFID 1.0

- Intelligent barcode
- Static
- Single purpose
- One Access Point
- Auto ID
- Limited security
- Use in Supply Chain



RFID 2.0

- RFID as a computer
- Dynamic
- Context aware
- Multiple Access Points
- Collaborative usage
- Rich security
- Use in full Product Life Cycle

- Prevent unauthorised access to RFID
 - Access Control functionality on the RFID itself
 - RFID only answers to authorised requests

- Differentiated access to data on the RFID
 - Memory to be structured in areas with individual access rights
 - Differentiate on read-only, write, delete etc.

- Communication between Reader and RFID should be unique for each transaction, to prevent eavesdropping, record & replay etc.

- Prevent RFID's from being cloneable

- Is there a need for standardization on enhanced RFID Security & Privacy ?
- If, then when is the right timing ?
- And if, then please keep standardization on a "semantic level", to open up for diversification and especially to open up for new innovation !

Thank You

- Questions ?



RFIDsec
Rued Langgaardsvej 7, 5te
DK-2300 S Copenhagen
Telephone: +45 39169444
E-mail: info@rfidsec.com
Web: www.rfidsec.com