Legal Aspects of RFID Technology

Jürgen Müller
University of Kassel
Provet – Project Team for
Constitutionally Compatible Technology Design

Matthias Handy
University of Rostock
Institute of Applied Microelectronics & CS

"Living in a Smart Environment"

- Interdisciplinary international research project
  - EE, CS, Law, Econ.
  - 7 universities (Germany, Switzerland)
- Implications of Ubiquitous Computing
- Funded by Daimler-Benz-Foundation, Ladenburg
- http://www.smart-environment.de (in german)
- http://www.daimler-benz-stiftung.de (english)

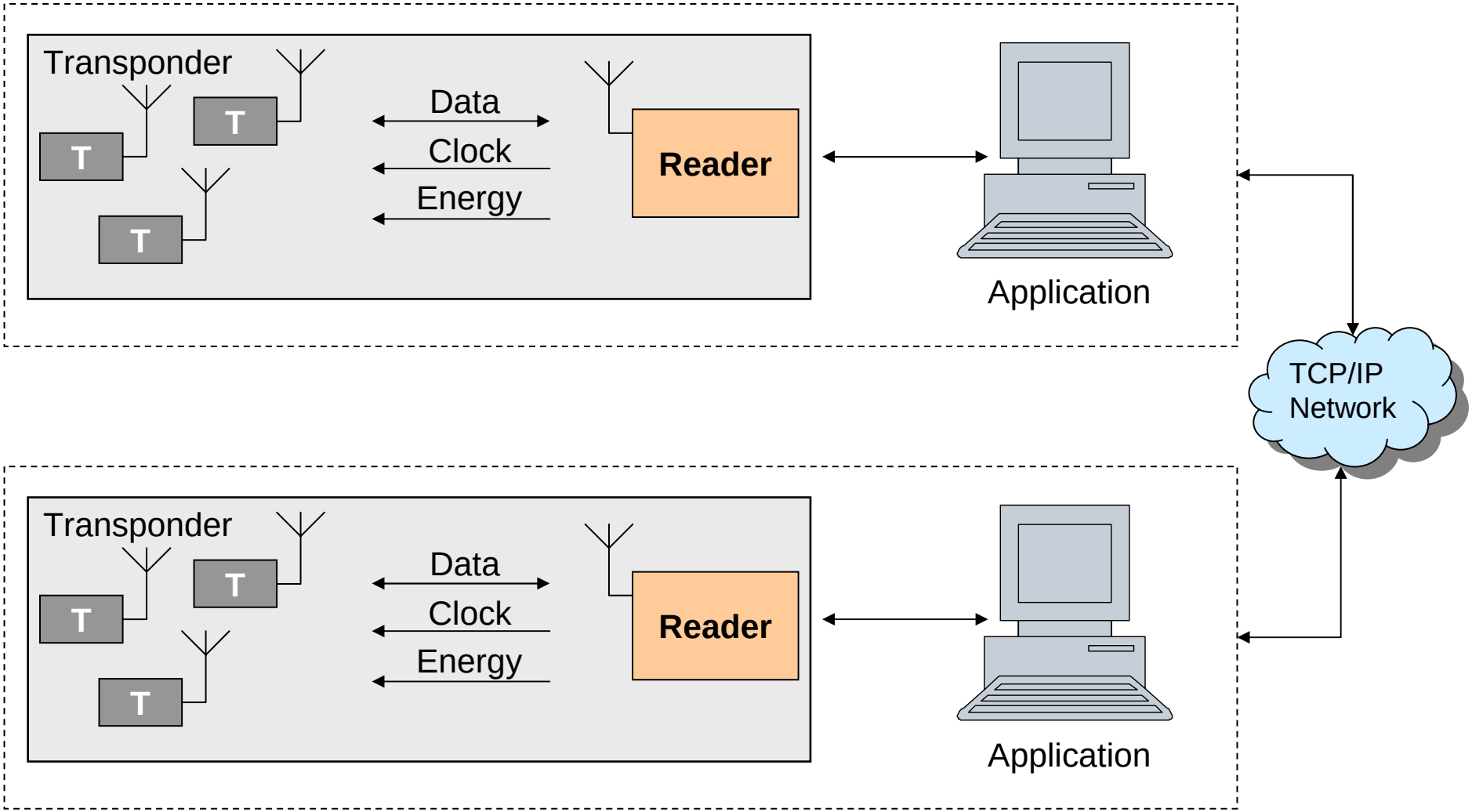
Motivation

- A hype about RFID technology
- Published (and public) opinion is critical
  - Feb.2004: Protest at Metro FutureStore
  - 20-30 participants; worldwide headlines on TV, newspapers, Internet
- Main questions
  - Are there legal issues in the use of RFID technology?
  - How can privacy issues be solved (and consumers be conviced)?

Agenda

- Introduction
- Scenarios of RFID-applications
- Legal relevant application constellations
- Survey of applicable regulatory systems
- Need for protection
- Technical solutions
- Outlook

Elements of an RFID-System



Application Examples

Constellation:

- Goods with RFID-tags in retail stores as a customer information system
- RFID-tags given to customers as a customer card
- Packaged goods and packaging with RFID-tags for internal logistic requirements

Application Example:

- Milk cartons
- Payback Card
- Suitcase

Application Constellation

From a legal point of view there are three main areas of relevance with respect to the use of RFID-Systems:

RFID-tags as a means of identification and a means of information storage ...

… attached to objects and used by third parties (Constellation 1)

… issued to the customer and used solely by the issuer or a third party (Constellation 2)

… used for internal or merely bilateral purposes (Constellation 3)

Overview: Legal Classification + Subsumtion (1)

Applicable regulatory system:

Constellation 1	
TC-Law	(-): E-Communication Framework-DIR (2002/21/EC), (-): bugging prohibition in PEC-DIR (2002/58/EC, Art. 5 I) because those regulations are only applicable for publicly available electronic communications services (-) TKG, except for bugging prohibition § 89 TKG Unless RFID reading device is not in user's property and has a communication interface (e.g. WLAN IEEE 802.11) that is able to transmit data to a mobile device (e.g. PDA) of the user.

Overview: Legal Classification + Subsumtion (2)

Constellation 1*	
Multimedia Laws	Identifier Data: (-) E-Commerce-DIR 2000/31/EC; (-) TDG Non-Identifier Data: (+) E-Commerce-DIR 2000/31/EC; (+) TDG Unless there is no provider-user-relationship (e.g. in employer-employee relationship, recital no. 18 of EC-Dir)

* Provided that:

Directive 2000/31/EC bases on the conception of technological openess for information society services, and provided that RFID-tags will contain links to Intra- or Internet addresses (e.g. ONS) and in the long run possibility of RFID-tags storing data in multimedia form

Overview: Legal Classification + Subsumtion (3)

Constellation 1	
Data Protection Law	Identifier Data: (+) Data Protection-DIR 95/46/EC; (+) BDSG Non-Identifier Data: (+) Data Protection-DIR 95/46/EC, (+) TDDSG; (+) BDSG Limitation of scope: § 1 I Nr. 1 & 2 TDDSG (-) PEC-DIR 2002/58/EC, because there is no electronic communication service Only applicable for publicly available electronic communications services in public communications networks, Art. 3 I PEC-DIR 2002/58/EC, recital no. 10; Scope of DP-DIR 95/46/EC: applicable for non public communications services

Overview: Legal Classification + Subsumtion (4)

Constellation 2	
TC Law	(-) Framework-DIR (2002/21/EC) (-) bugging prohibition PEC-DIR 2002/58/EC, Art. 5 I (-) TKG, except § 89 TKG
Multimedia Law	Identifier: (-) E-Commerce-DIR 2000/31/EC; (-) TDG Non-Identifier: (-) E-Commerce-DIR 2000/31/EC; (-)TDG
Data Protection Law	Identifier: (+) DP-DIR 95/46/EC; (+) BDSG Non-Identifier: (+) DP-DIR 95/46/EC; (+) BDSG The transparency requirements of Art. 12 a) subsection 3 of DP-DIR 95/46/EC and of § 6c BDSG are not applicable because RFID-tags are not yet able to „use“ or „change“ data

Overview: Legal Classification + Subsumtion (5)

Constellation 3	
TC- Law	(-) Framework-DIR 2002/21/EC, (-) bugging prohibition PEC-DIR 2002/58/EC Art. 5 I (-) TKG, except § 89 TKG
Multimedia Law	Identifier: (-) E-Commerce-DIR 2000/31/EC; (-) TDG Non-Identifier: (-) E-Commerce-DIR 2000/31/EC; (-) TDG
Data Protection Law	Identifier: (+) DP-DIR 95/46/EC; (+) BDSG Non-Identifier: (+) DP-DIR 95/46/EC; (+) BDSG

Technologically determined possibilities (1)

Considering the features of RFID technology, these are the novel possibilities:

Technical Features	Possibilities
Radio interface	Sightless communication
Extremely small sizes	Unnoticeable placement on and in objects
Flexible materials	Undetachable and cheaply integrated into object

Worldwide unique identifier	Identifiability of RFID-tag

Store for non-identifier data (optional)	Content identity

Integration into a background information system (e.g. ONS)	Unlimited additional and context data about an object

Technologically determined possibilities (2)

Technical Features	Possibilities
No input or output medium apart from reader	Unregistrability of the processes
No access protocol	

No access protection	Open data and communication
No data protection	
No communication protection	

Limited radio range	Controllability in the radius of the range

Risks of RFID-Systems (1)

Overview of Risks in the Use of RFID-Systems

- Imperceptibility of Presence
- Imperceptibility of Data Processing Sequences Taking Place
- No Control in Use of Object
- Omnipresence of Use
- Integration of Data Processing Processes into Behaviour and Actions of the Party Concerned
- No Escape from the Data Processing Processes

Risks of RFID-Systems (2)

- Object Related Data Traces (e.g. Movement Profile via Site Date of Reader)
- Object Related Context Data
- Higher Validity of Context Data
- Capacity for Re-recognition and Assignment of Object
- Capacity to Indentify and Read Patterns (Sequences and Habits) by Relationalization of Objects Detected
- Generation of Valid Knowledge on Re-recognition on Re-recognition of Patterns via Additional Data
- Danger of Manipulation of Open Data and Communication

Potentially Violated Rights

Starting point: RFID-Systems are both Part of the Virtual Social World and the Real Physical World.

Thus, the following Rights could be violated:

- Protection of Proprietary Rights
  (Art. 14 GG, Art. II-77 Constitution for Europe (draft))
- Protection of Freedom of Action
  (Art. 2 I GG, Art. II-66 Constitution for Europe (draft))
- Protection of Confidentiality of the communications or telecommunication privacy
  (Art. 10 GG, Art. II-67 Constitution for Europe (draft), Art. 8 EHRC)
- Protection of personal datas and informational self-determination
  (Art. 1 I, 2 I GG, Art. II-68 Constitution for Europe (draft))

Need for Protection (1)

To guarantee telecommunications privacy (Art. 10 GG), personal data-protection and informational self-determination (Art. 1 I, 2 I GG), protection is necessary.

Protection Programme that has to be incorporated:

Proprietary Right (§ 903 BGB) and Possession (§ 872 BGB)

- Guarantee removal and deactivation rights
- No removal or deactivation rights in the case of temporary possession of property (e contrario § 872 BGB), because this is no interference with possession (§ 858 BGB)

Technical and Organizational Protection Measurements according to § 9 BDSG, DP-DIR 95/46/EC Art. 17

- Securing Transponders against Bugging by Third Party
- Securing Data against Unauthorized Access and Manipulation

Need for Protection (2)

Transparency Principle

(DP-DIR 95/46/EC Art. 10, Art. 11 and Art. 12)

- Knowledge about use of RFID Systems
- Knowledge about type and content of processed data
- Knowledge about structure of data processing processes (also integration of data processing processes in a background information system, e.g. ONS)
- Knowledge about use of data gathered by RFID Systems

- Perceptibility of Sequence of Data Processing Procedures
- Perceptibility of the Communication Processes between RFID tag and Reader

- Perceptibility of the Purpose of the stored Data
- Perceptibility of Designation of Data Recipients

Need for Protection (3)

Purpose Determination (DP-DIR 95/46/EC Art. 6, I b)

- Exclusion of Storage and Use of Data Recorded by RFID-tags, expecially for Commercial Use

Informational Division of Powers (DP-DIR 95/46/EC Art. 6, I b)

- Hermetic Protection of Data according to their Purpose Determination Entailing Separation of Data in the RFID-tag Identifier with Serial Number Function of Data with Content Determination

Data Avoidance (§ 3a BDSG, DP-DIR 95/46/EC Art. 6 I c)

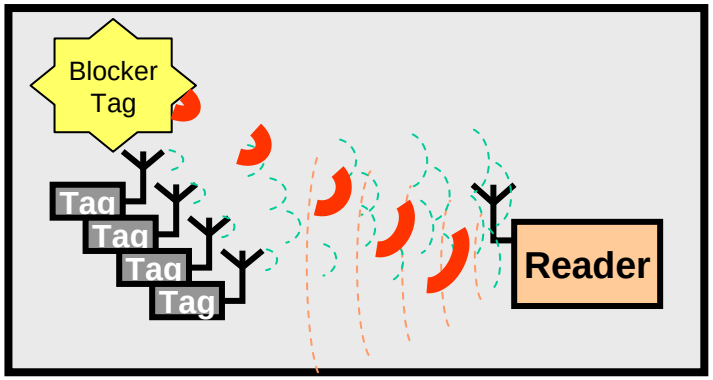
- Preventive Measures in the context of RFID application must be taken
- This contains also the Requirement to enable Deactivation or Removal of RFID-tags because they are potential Data Processing objects

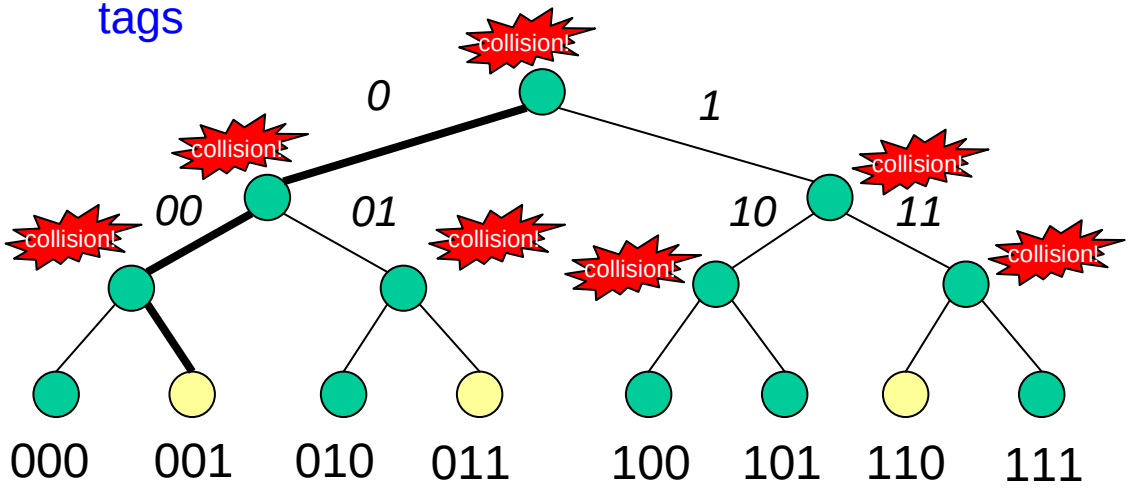
Solutions – Technical Approaches

- Existing Approaches:
  - Blocker-Tag, Kill-Command, Meta-ID, Jamming
- Alternatives:
  - Delete serial number; only object class remains on tag (same as bar code)
  - Replace serial number with private (variable) inventory number
  - break logical connection: RFID-Tag ←→ Object
    - RFID-tag stores object's identity as bit sequence
    - "Real" identity after decoding (look-up)
    - Delete database entry of an object
    - Limit access to look-up-service

Anticollision: Blocker Tag

- A. Juels, R. Rivest, M. Szydlo; 2003
- (Selective) Blocking of RFID tags
- Only works with binary search anticollision
- Simulates the full set of 2^k possible RFID-tag serial numbers
- Reader cannot tell which tags are really present
- Example: 48 bit ID, Reader reads 1000 tags/s: > 8000 years reading all tags





Anticollision protocol recursively asks:

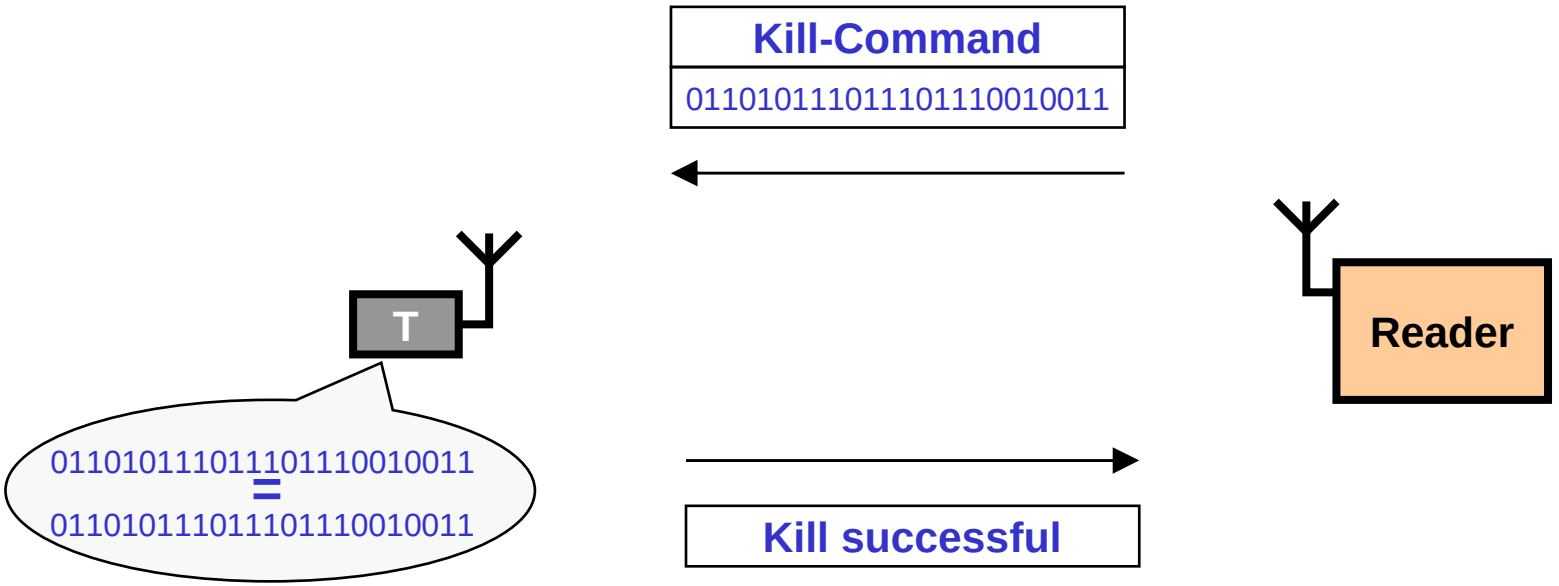
"What is your next bit?"

Blocker tag always answers:

"Both 1 and 0!"

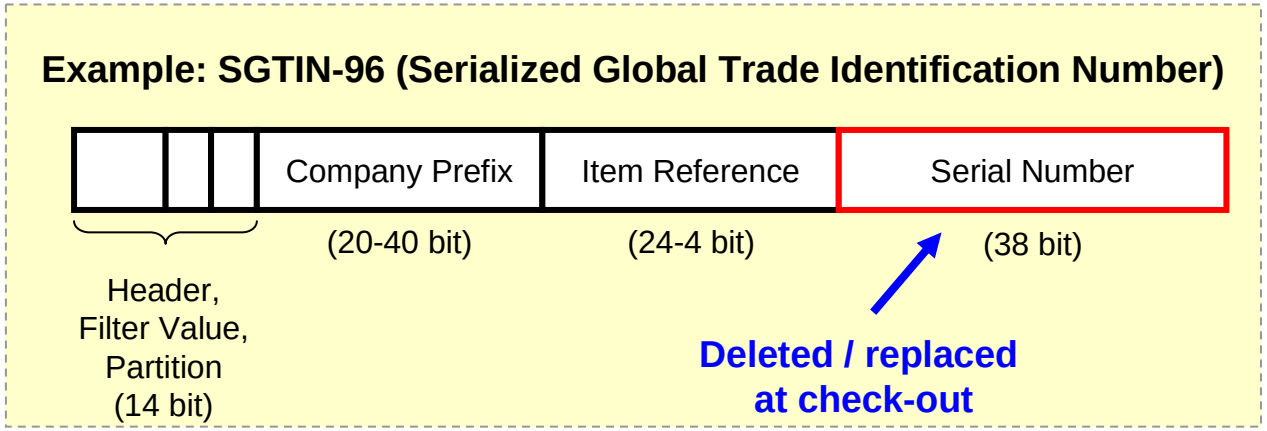
Kill-Command

- As defined in EPC Protocol Specification for 900 MHz Tag
- Permanently disables a tag
- Kill command carries 24-bit passcode
- If command's passcode matches tag's passcode → tag is killed



Replace Serial Number

- Drawback of the Kill-Command → "Smart Appliances" won't work
- Better Approach: Delete or replace serial number; item reference (object class) remains
- Replace unique serial number with private inventory number
- Problem: Tracking



Meta-ID*

- Tags able to store Meta-ID
- Owner can lock a tag:
  - Computes hash-value of random key
  - i.e. *lock = hash(key)*
  - Tag stores lock-value and enters locked state
- To unlock tag:
  - Owner sends original key value to tag
  - Tag hashes key and compares it to stored value
  - If match → tag unlocked
- A locked tag only responds with its Meta-ID!
- Problem: Tracking → Refresh Meta-ID!

* Sarma et al., 2002

Application Identifier (AI)

- Indicates **target application** of RFID-tags (e.g. logistics)
- Reader includes AI in request
- RFID-tag only answers if $AI_{Reader} = AI_{Tag}$
- AI can be locked by "owner"
- No AI in reader request → **No tag will respond!**
- In ISO 15693:
  - 8-bit AFI (Application Family Identifier)
  - Reader transmits AFI with Inventory-Command
  - Tags with different AFI don't respond
  - No AFI in request → **All tags in range will respond!**

Data Usage Identifier (DUI)

- Indicates intended **data usage** of RFID-Tag
- Assumption: Tag-ID not relevant; tag memory contains personal data
- Reader requests information → tags respond with Tag-ID and DUI
- With DUI the user has to decide to acquire more data from a tag
- ISO/IEC 15693:
  - DSFID: Data Storage Format Identifier

Results (1)

Increase of risks with RFID usage, if there is:

- Increase of computational and storage capacity
- Integration of sensors
- Integration into networks
- "Better" energy supply for RFID tags

The following apply to RFID systems:

- RFID systems are not per se a threat for privacy.
- Many regulations of existing data protection law can be applied.

Results (2)

Objectives might be :

- Extended transparency regulations for RFID systems in multimedia law
- Extended transparency regulations for RFID systems in data protection law (latitude for member states DP-DIR 95/46/EC recital 53)
- Obligation to be able to deactivate RFID tags
- Strengthening of preventive action in data protection law

Data protection should be concerned more with **prevention**, because with the use of RFID systems the interests of people only come into play when a lot of already processed data can be accessed.

Outlook

Alliance between Technology und Law: