"Adoption of RFID – An Introduction to the Technology and Review of Technology Acceptance Studies"

Ringvorlesung "Anwendungen der Informatik"
May 2006

Dr. Sarah Spiekermann
Humboldt-Universität zu Berlin

Agenda

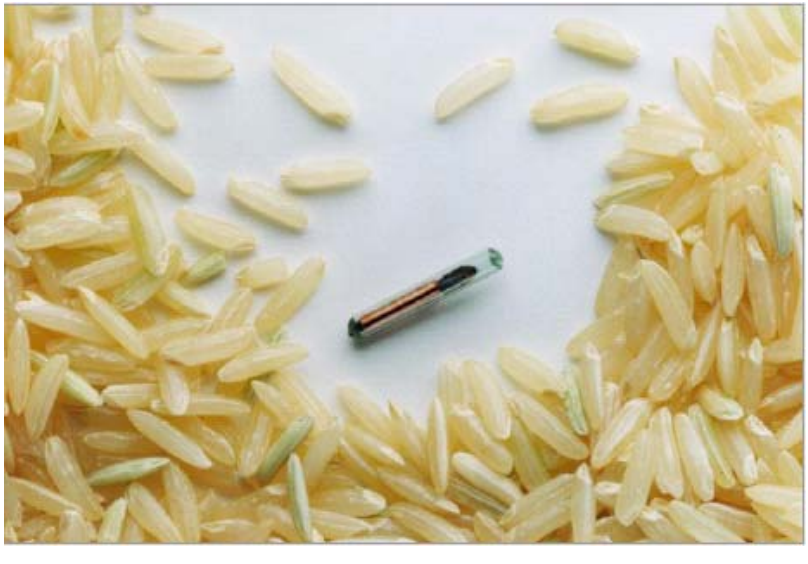
- **RFID: An Introduction into the Technology**
- **Consumers‘ View surrounding RFID**
- **Technical Feasibility of Consumer Fears**
- **A 7-Point Plan to Ensure Privacy**

Agenda

- **RFID: An Introduction into the Technology**
- **Consumers‘ View surrounding RFID**
- **Technical Feasibility of Consumer Fears**
- **A 7-Point Plan to Ensure Privacy**

RFID (= Radio Frequency IDentification) tags will be embedded in most objects in the future.

Not all RFID tags are equal



- **Electronic tags refer to a family of technologies that transfer data wirelessly between tagged objects and electronic readers.**
- **Radio Frequency Identification (RFID) tags transmit data over a short range. Important distinctions:**
  - Active vs. Passive tags
  - Tag Classes
  - Tag Generations

Depending on the frequency used RFID tags have very different read ranges.

Reichweiten: Passive Tags

Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
6,75 MHz	-	44 Meter	1 Meter	Induktive Koppelung
13,56 MHz	Früher Supply – Chain – Management (Trend geht zu UHF)	3,5 Meter	1 Meter	Induktive Koppelung
UHF (865-928 MHz)	Supply – Chain - Management	unbegrenzt	7 Meter	Backscatter

Reichweiten: Aktive Tags

Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
UHF (868-928 MHz)	Mautsystem (z.B. in Österreich)	unbegrenzt	15 - 30 Meter	Backscatter

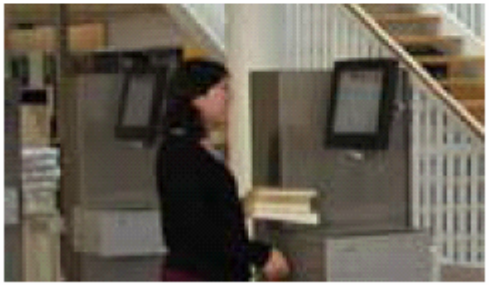
Tag Classes are being distinguished on the basis of tag capabilities.

Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift Tags	None	Passive	Article Surveillance
1	EPC	Read-Only	Any	Identification Only
2	EPC	Read-Write	Any	Data Logging
3	Sensor Tags	Read-Write	Semi-Passive or Active	Environmental Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc Networking

Quelle: Weis, Security and Privacy in Radio-Frequency Identification Devices

RFID tags have been in use for a long time.

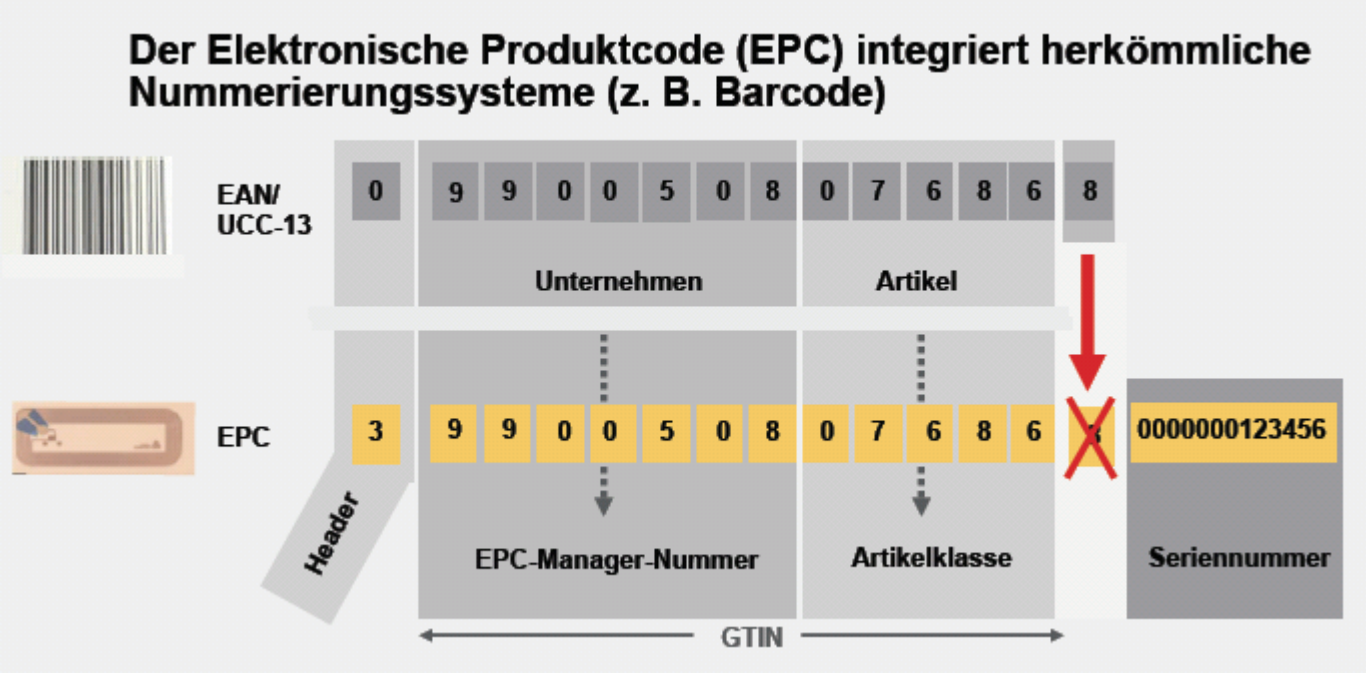
Skipass mit integriertem RFID-Chip



Bibliotheksausleihe mit RFID

Düsseldorf-Marathon mit RFID

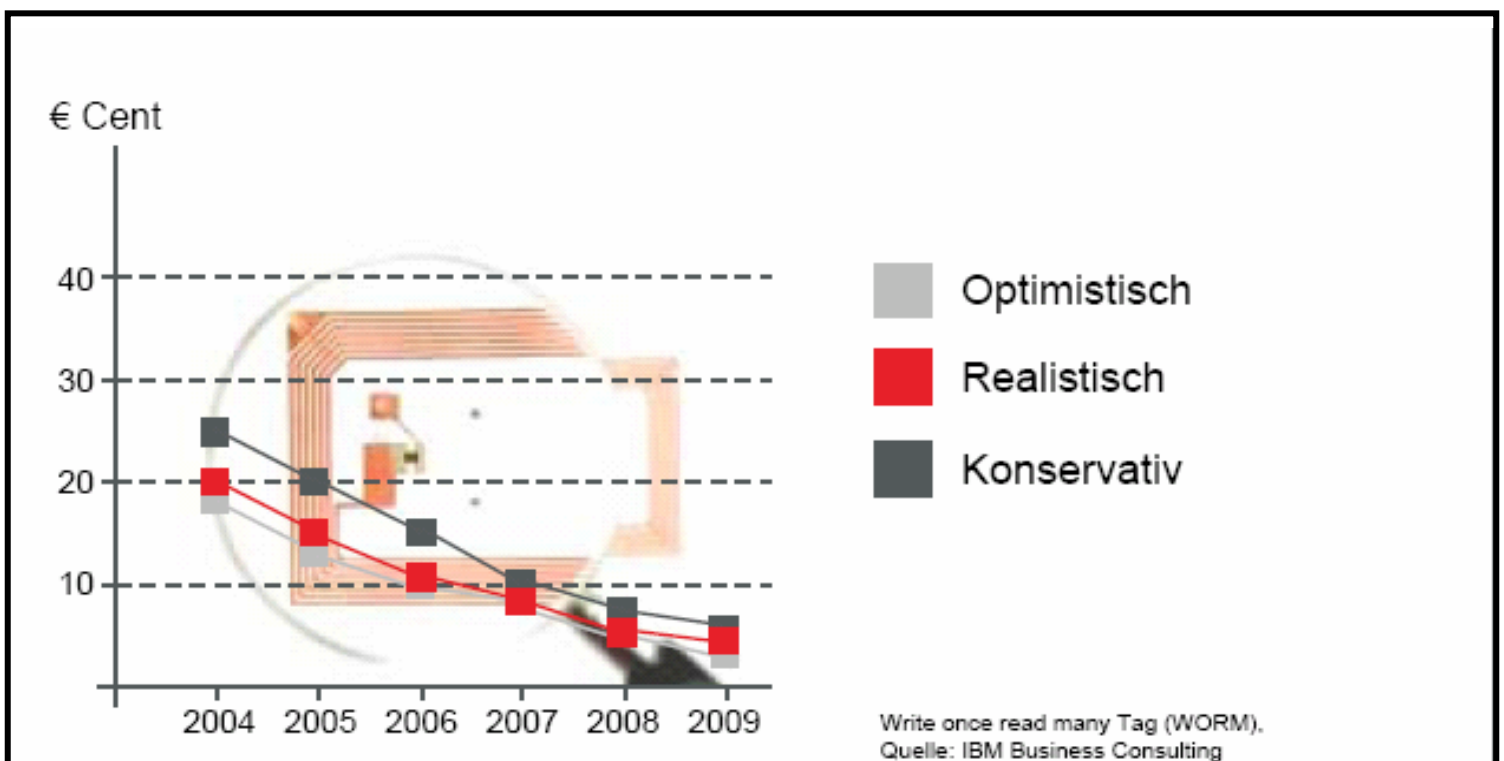
The Electronic Product Code (EPC) uniquely identifies each object.



The EPC code was intended to be universally and globally accepted as a means to link physical objects to the computer network/to serve as an efficient information reference.

Quelle: „RFID Fahrplan der Metro Group", Dr. Gerd Wolfram, RFID-Kongressfür die Partner der METRO Group , Köln, 14. Mai 2004

RFID tag cost is declining to a point where item level tagging becomes economically realistic even for low value products.



Quelle: „RFID Fahrplan der Metro Group", Dr. Gerd Wolfram, RFID-Kongressfür die Partner der METRO Group , Köln, 14. Mai 2004

However, RFID tags as we know them are only *one* component of the *Intelligent Infrastructure*.

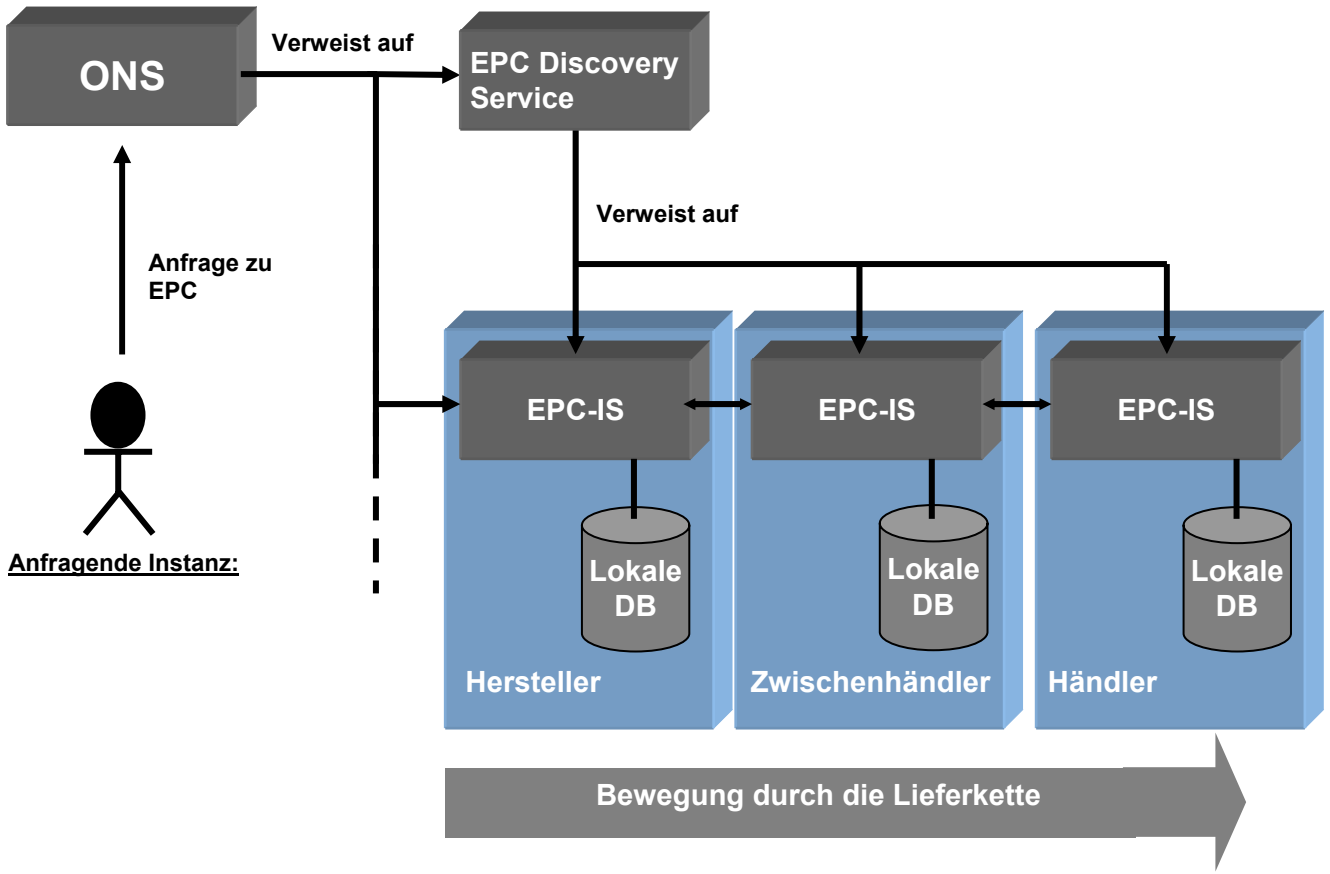
Components of the Intelligent Infrastructure

- Electronic tags (e.g. RFID tags)
- Electronic Product Code (EPC)
- Physical Markup Language (PML)
- Object Naming Service (ONS)
- EPC Discovery Service

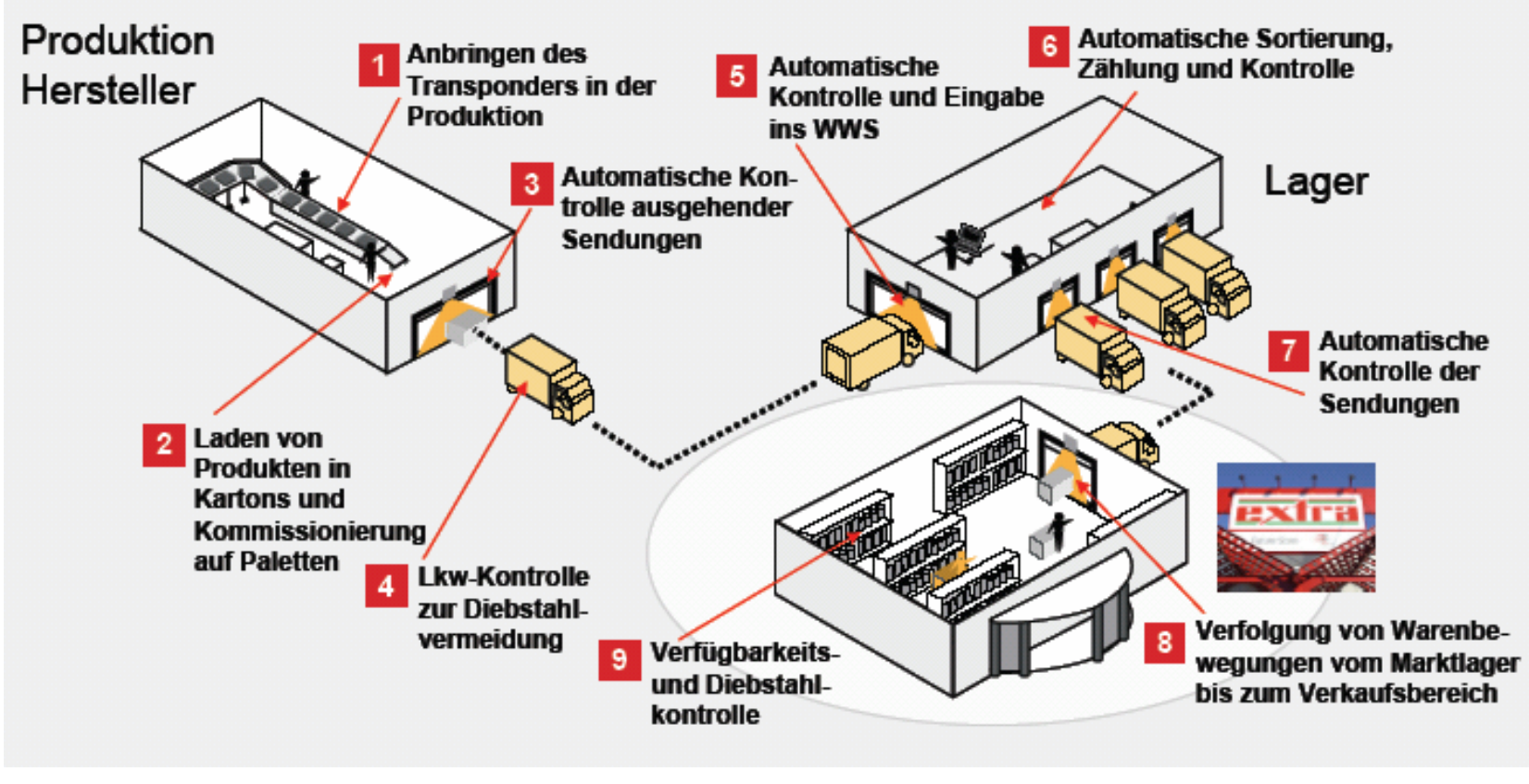
The Physical Markup Language (PML) is intended to be the standard in which networked information about physical objects is written.

- **Physical Mark-Up Language (PML)**
  - **Based on XML**
  - **Description of physical objects**
  - **Independent of transport protocols and applications**
- **PML-Core (Schema)**
  - **Facilitates data exchange**
  - **Standardizes information, e.g. place, time, date, measures, etc.**
- **PML-Extensions**
  - **Application specific schemata**

The Object Naming Service (ONS) is the 'glue' which links the Electronic Product Code (EPC) with its associated data file (accessible via EPC-IS).



RFID Tags are supposed to be used at many points of the supply chain.



Quelle: „RFID Fahrplan der Metro Group", Dr. Gerd Wolfram, RFID-Kongressfür die Partner der METRO Group , Köln, 14. Mai 2004

Agenda

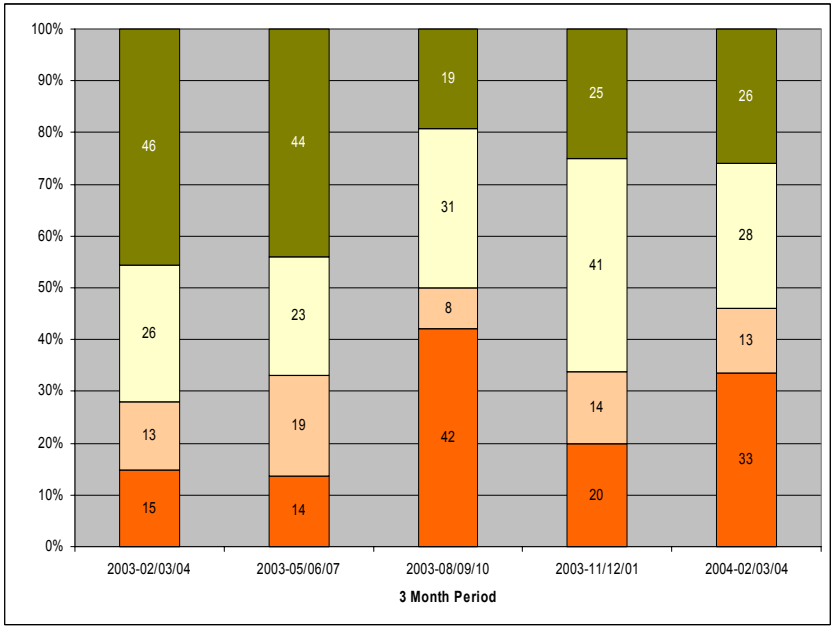
- RFID: An Introduction into the Technology
- **Consumers‘ View surrounding RFID**
- Technical Feasibility of Consumer Fears
- A 7-Point Plan to Ensure Privacy

RFID introduction has stirred some concern by privacy rights organisations.

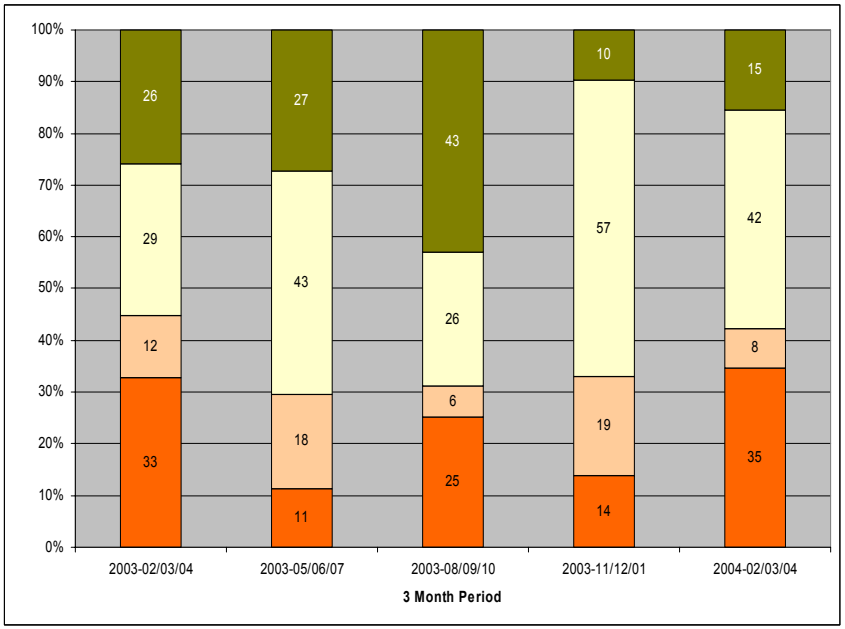
Demonstration in Rheinberg

Consumer fears associated with RFID chips have become an 'issue' the mass media.

German Press



International Press

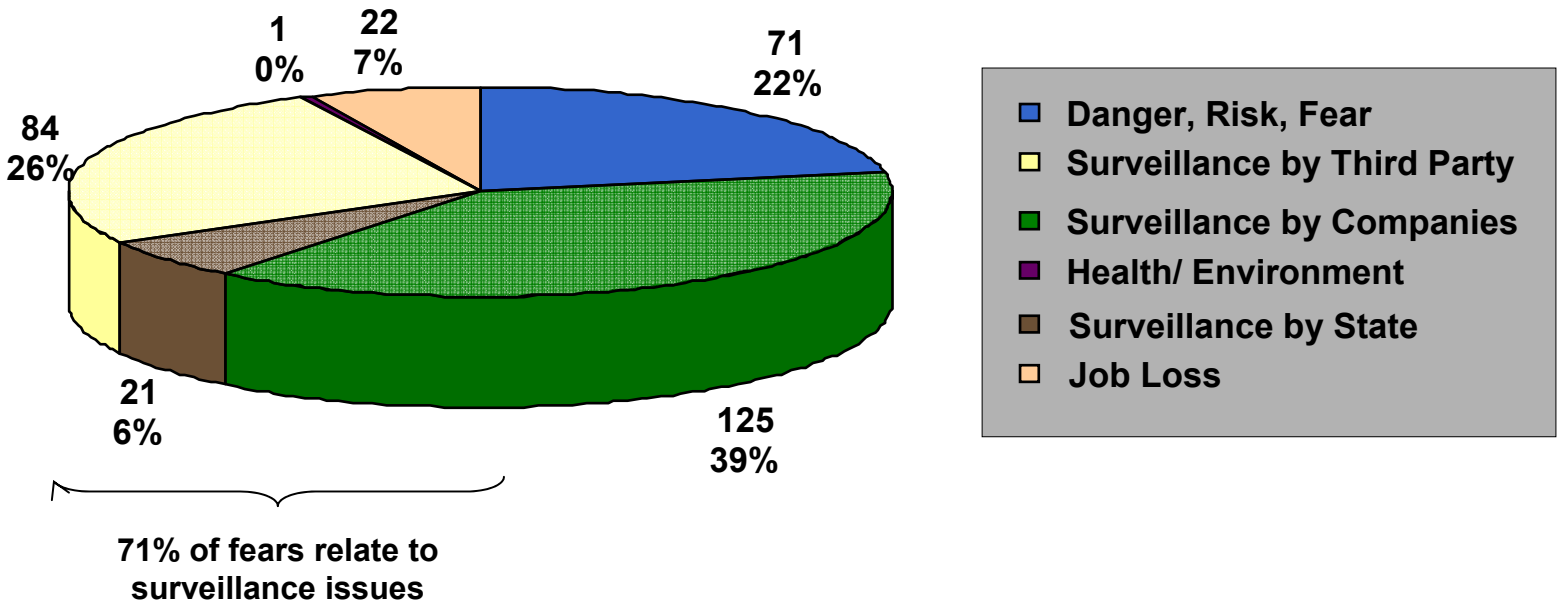


Consumer Benefits | Company Advantages
Consumer Fears | Company Disadvantages

*Base: 350 articles published between 2000 and 2004 were analyzed from 68 national and international sources.

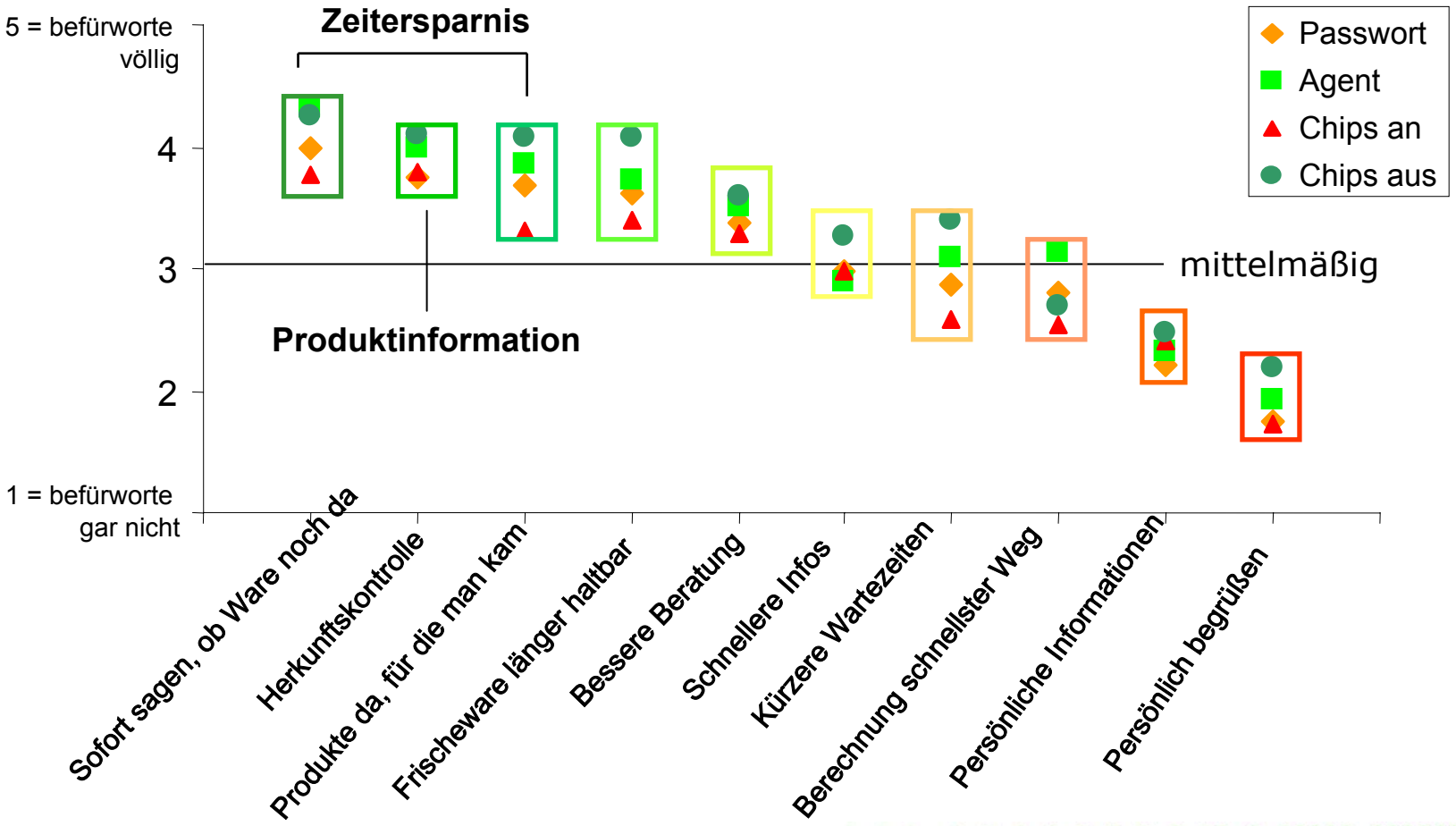
Within the 'fears' category, surveillance by companies is the major social challenge recognized for RFID technology.

Relative Importance of 'Fear' Types mentioned in German Popular Press: 2003/11 – 2004/04

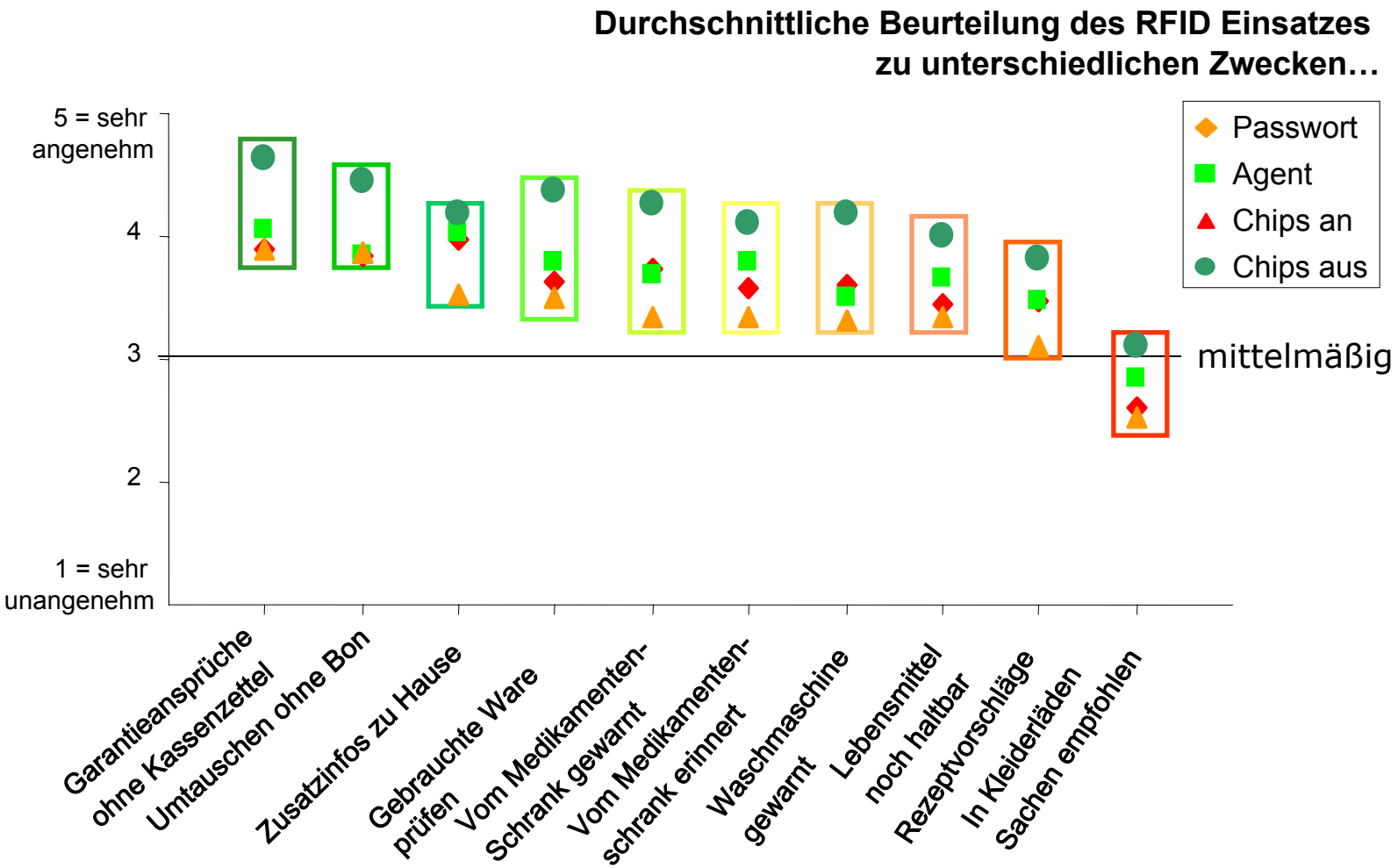


Benefits from RFID at the Point of Sale

Durchschnittliche Beurteilung des RFID Einsatzes zu unterschiedlichen Zwecken…



Benefits from RFID after purchase.



What are major consumer fears associated with RFID?

Focus Groups conducted for the Metro Group revealed 5 major threats.

1. Unauthorized readout of one's belongings by others
2. Tracking of persons via their objects
3. Retrieving social networks
4. Technology paternalism
5. Making people responsible for their objects

→ **Loss of Control**

Unfortunately, industry groups tend to play down the real threat of RFID.

GS1 (CCG): „RFID in the context of Consumer and Data Protection“ (Management Information Paper, April 2004)*

- „With an EPC transponder we continue to just store a non meaningful number“ (p.1)
- „In terms of process logic, nothing is being changed.“ (p.2)
- „RFID readers are expensive and will only be mounted where this makes sense, namely in retail outlets at the checkout, at the exit for theft protection and on shelves for stock-keeping reasons.“ (p2)
- „Even if transponders were being read out unauthorized, nobody can make use of the article or client number if one hasn‘t got the respective access to backend databases.“ (p.2)

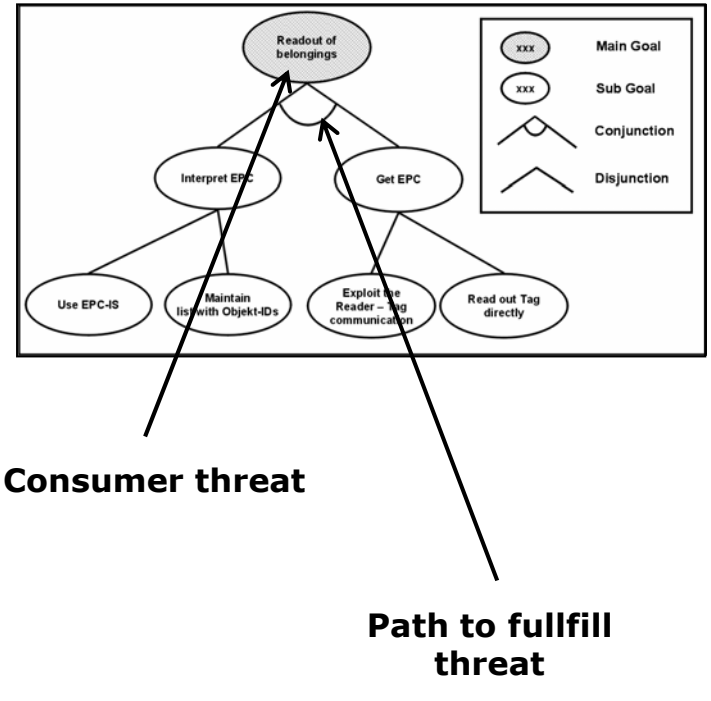
*own translation

Agenda

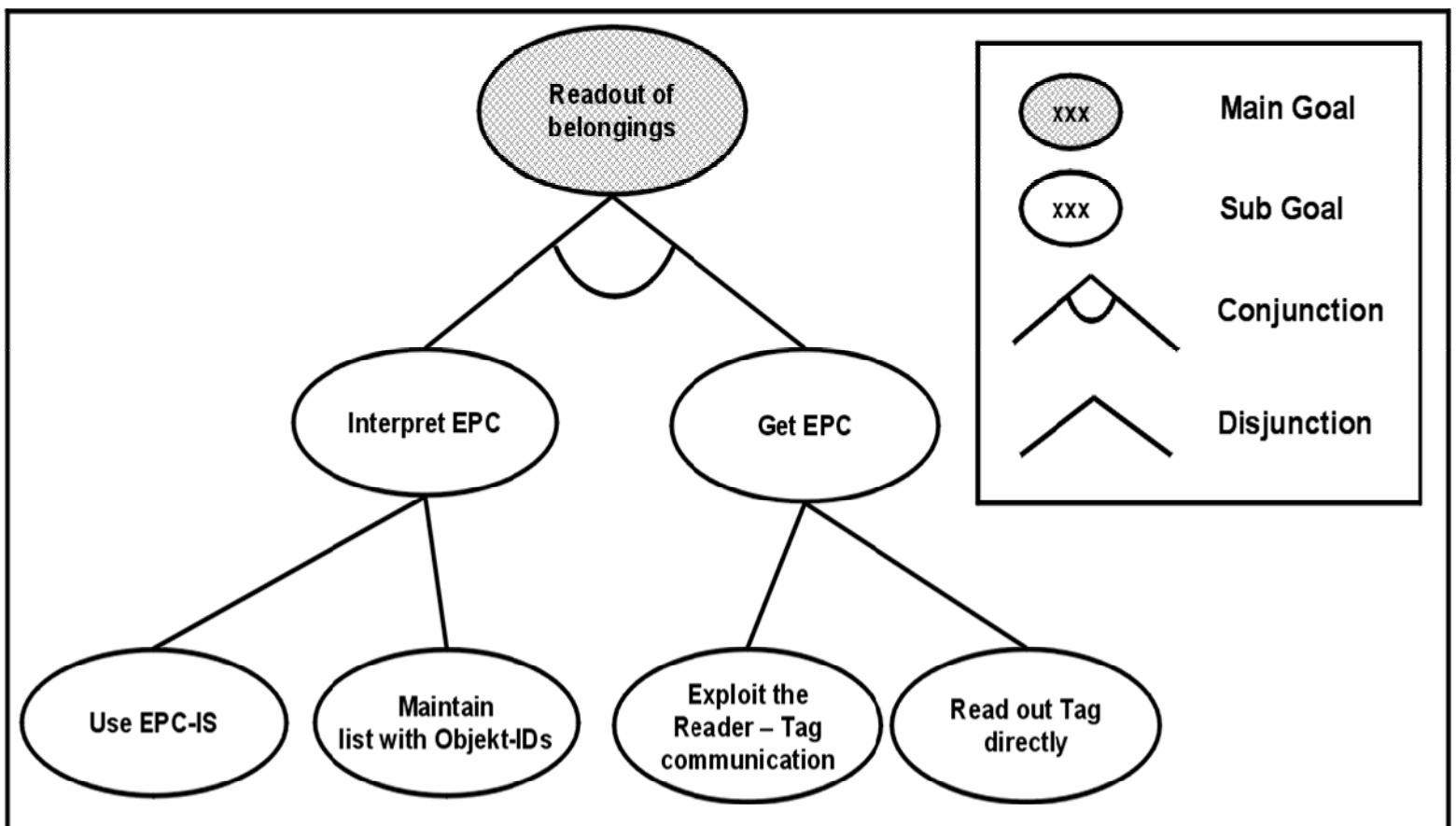
- RFID: An Introduction into the Technology
- Consumers‘ View surrounding RFID
- **Technical Feasibility of Consumer Fears**
- A 7-Point Plan to Ensure Privacy

Goal of the attack-tree analysis presented

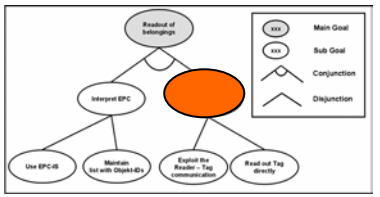
- Provide proof of the technical feasibility of consumer threats.
- Provide proof of economic sense behind potential implementation scenarios.
- Provide a basis for structured technical discussion to implement security and privacy.
- Create a document that is clear and complete for management information.



Unauthorized readout of one's belongings by others



Getting the EPC is easy if item level tags will operate on the UHF band.



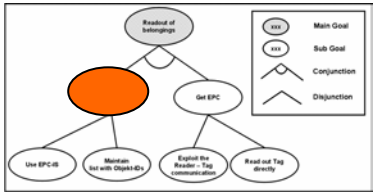
Reading Distance: Passive Tags

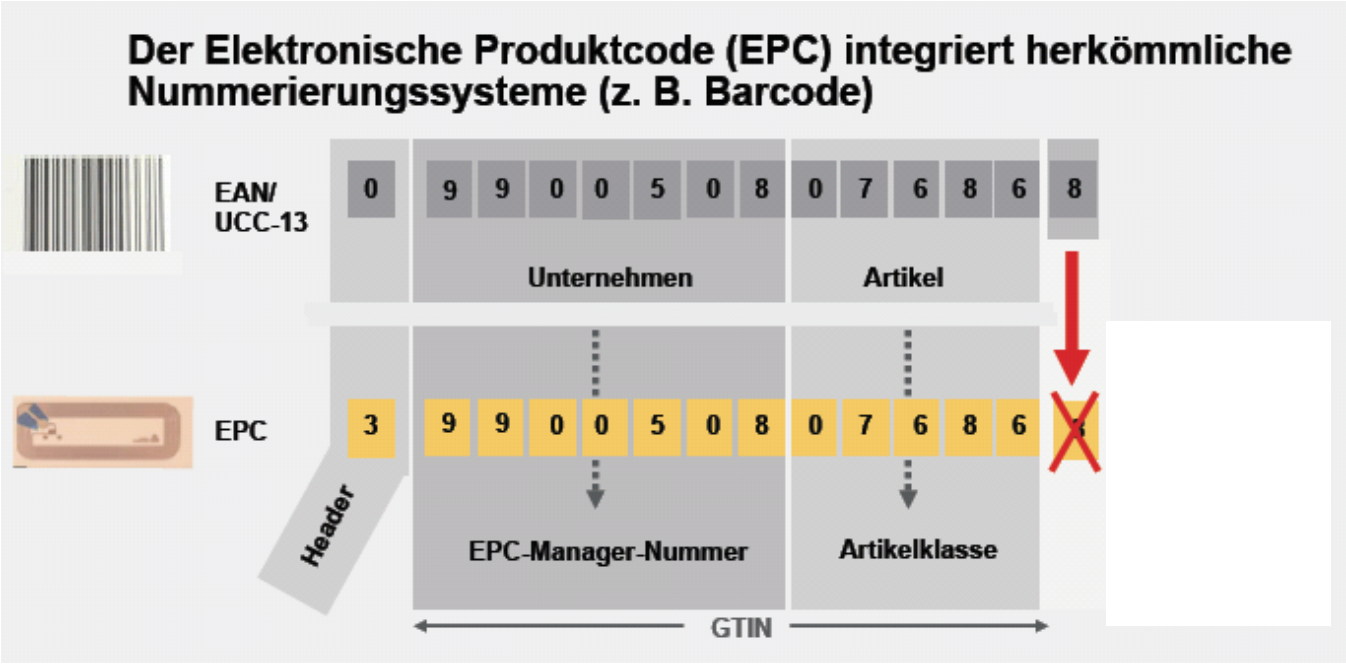
Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
6,75 MHz	-	44 Meter	1 Meter	Induktive Koppelung
13,56 MHz	Früher Supply – Chain – Management (Trend geht zu UHF)	3,5 Meter	1 Meter	Induktive Koppelung
UHF (865-928 MHz)	Supply – Chain - Management	unbegrenzt	7 Meter	Backscatter

Reading Distance: Active Tags

Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
UHF (868-928 MHz)	Mautsystem (z.B. in Österreich)	unbegrenzt	15 - 30 Meter	Backscatter

The Electronic Product Code (EPC) uniquely identifies each object.

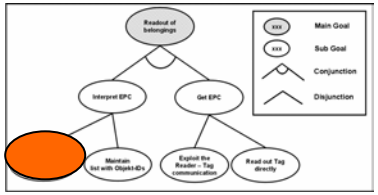


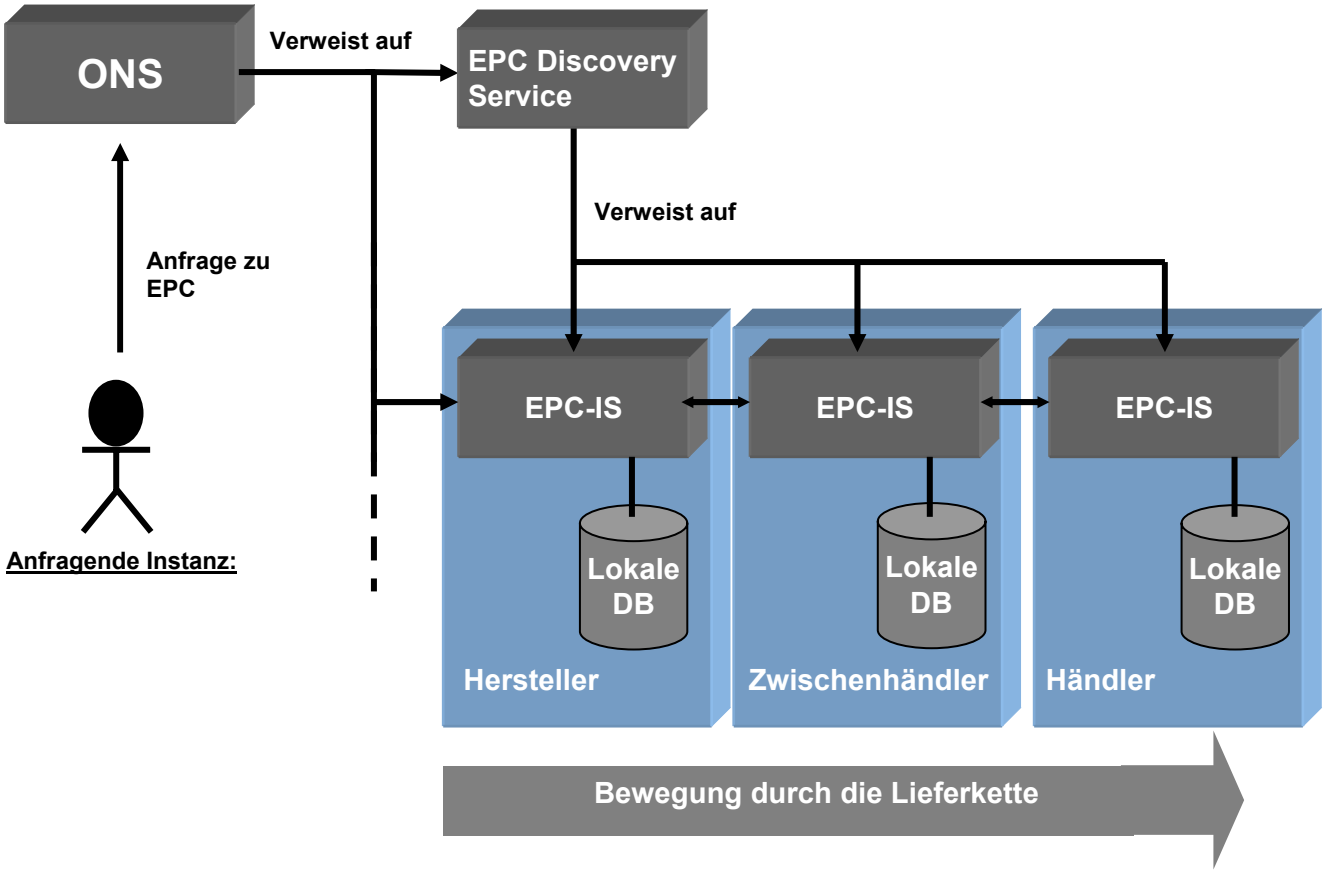


The EPC code was intended to be universally and globally accepted as a means to link physical objects to the computer network/to serve as an efficient information reference.

source: „RFID Fahrplan der Metro Group", Dr. Gerd Wolfram, RFID-Congressf for METRO Group partners , Cologne, May 2004

Object data is available for those having access to the EPC Network or to a local EPC-IS.

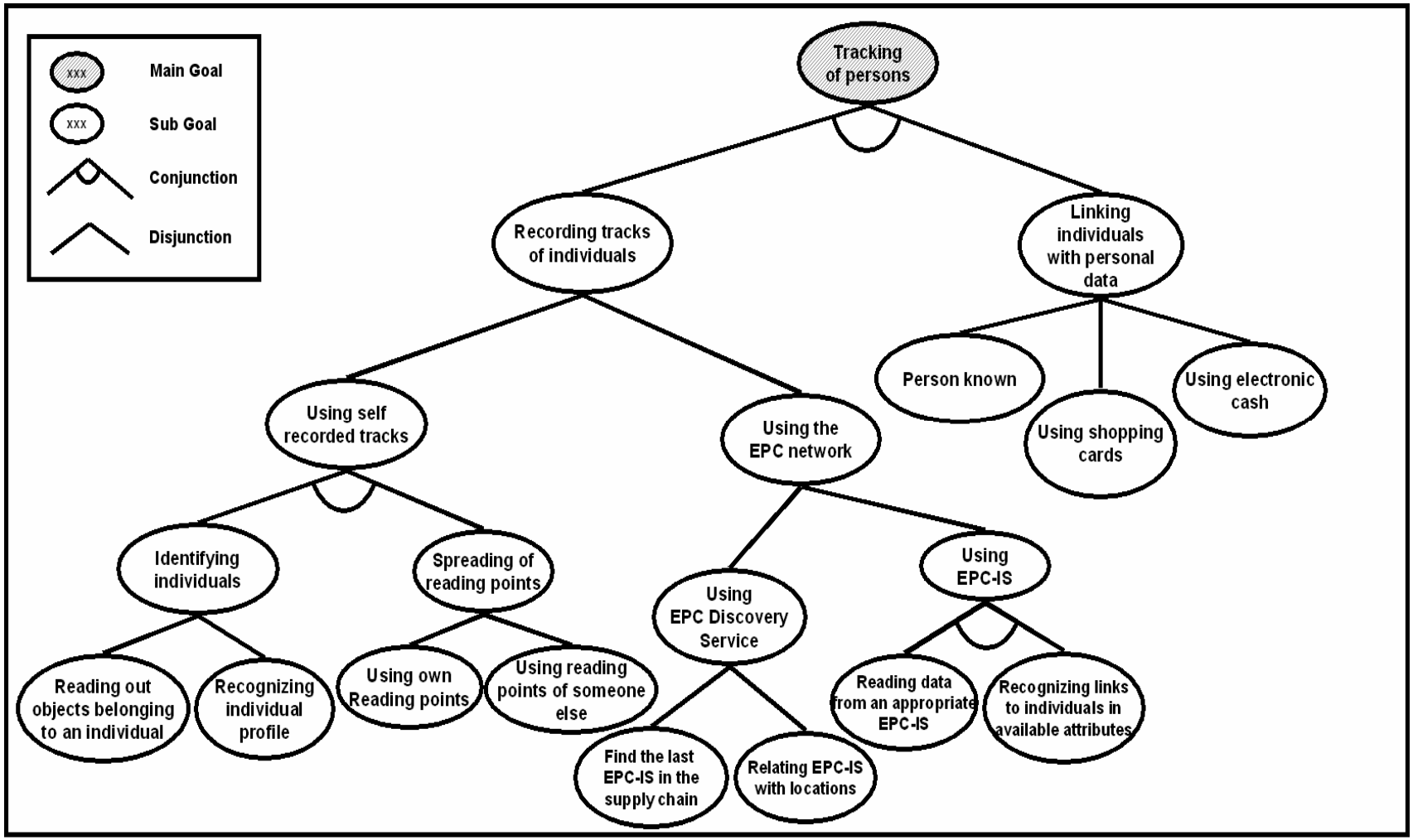




On this background, we suggest 3 privacy measures.

- Default killing of RFID tags at store exits OR password protection of RFID tag content.
- No sharing of local tracking data (times and places) with the EPC Network beyond logistics.
- Rigorous controls and transparency of EPC Network access rights.

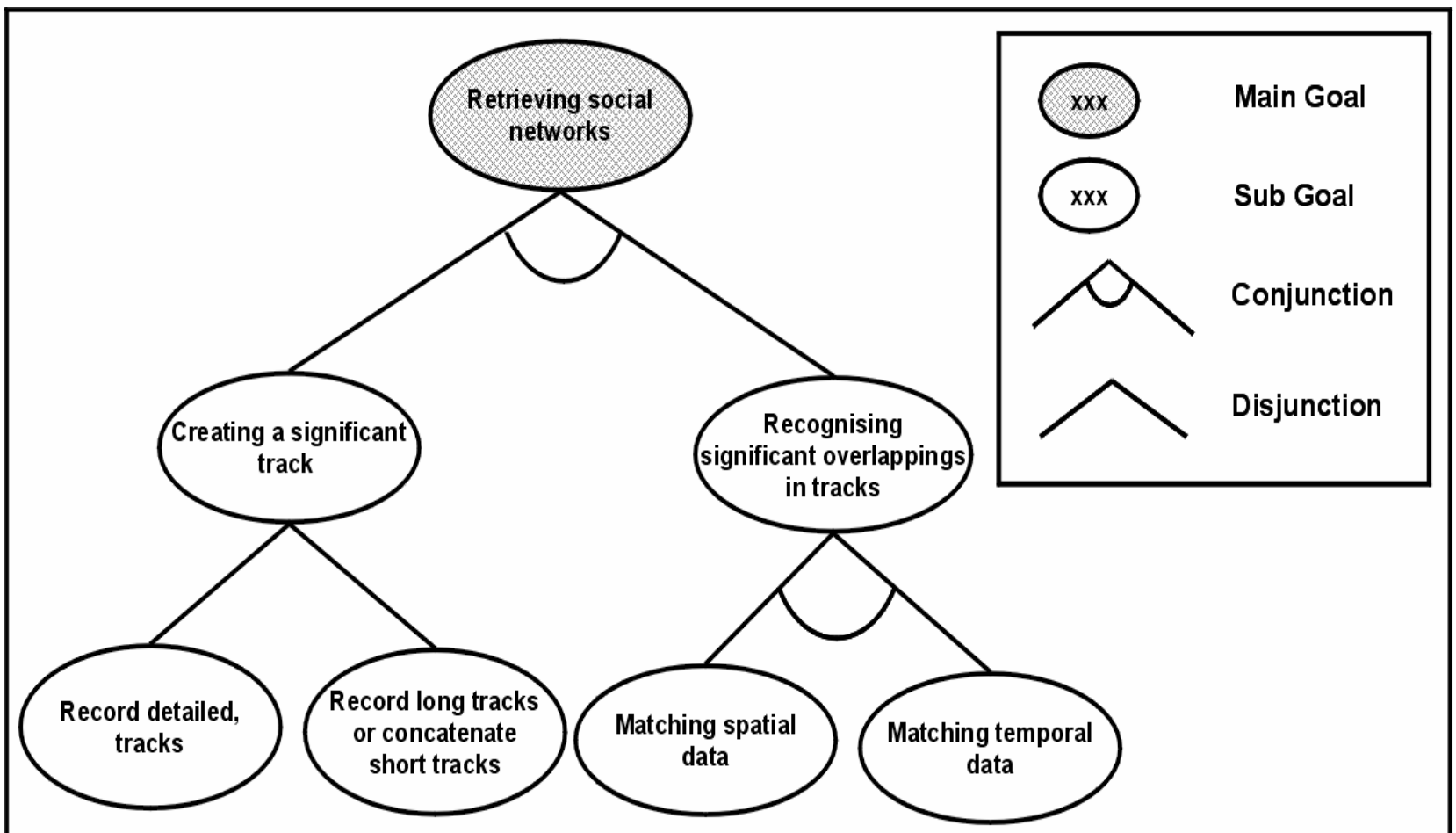
Tracking of persons via their objects



Only around 30% are fine with tracking in a retail outlet IF they get the fastest track calculated for them in return.

RFID Use	Positiv ---------- Judgement %---------- Negativ				
Fastest Track through the supermarket	9,3 %	22,2 %	18,5 %	13 %	37 %

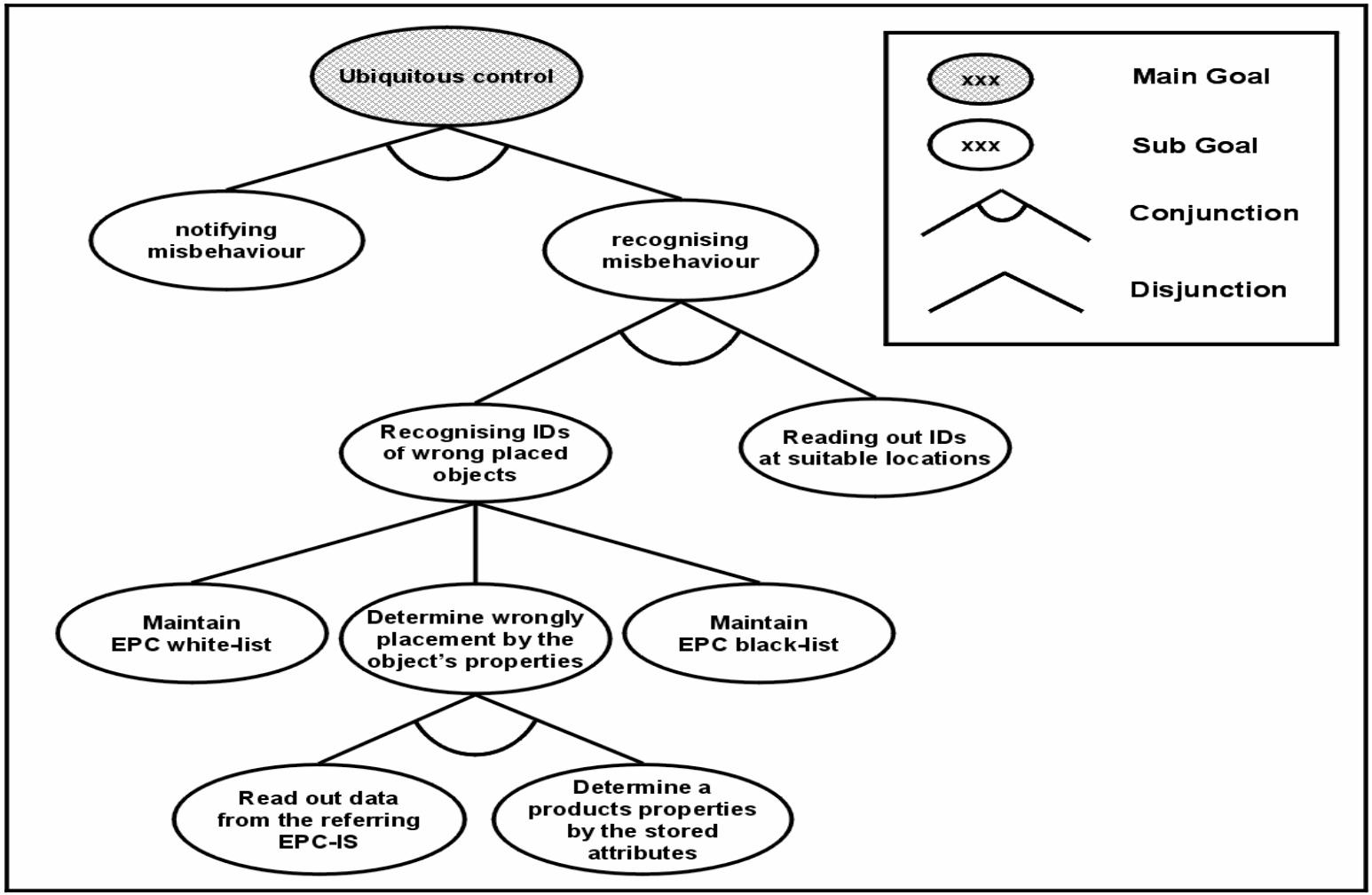
Retrieving social networks



On this background we added 2 further privacy measures.

- Default killing of RFID tags at store exits OR password protection of RFID tag content
- No sharing of local tracking data (times and places) with the EPC Network beyond logistics
- **Minimal granulariy: Limited timestamp information**
- Rigorous controls and transparency of EPC Network access rights
- **Deletion of all object data after a certain period of time**

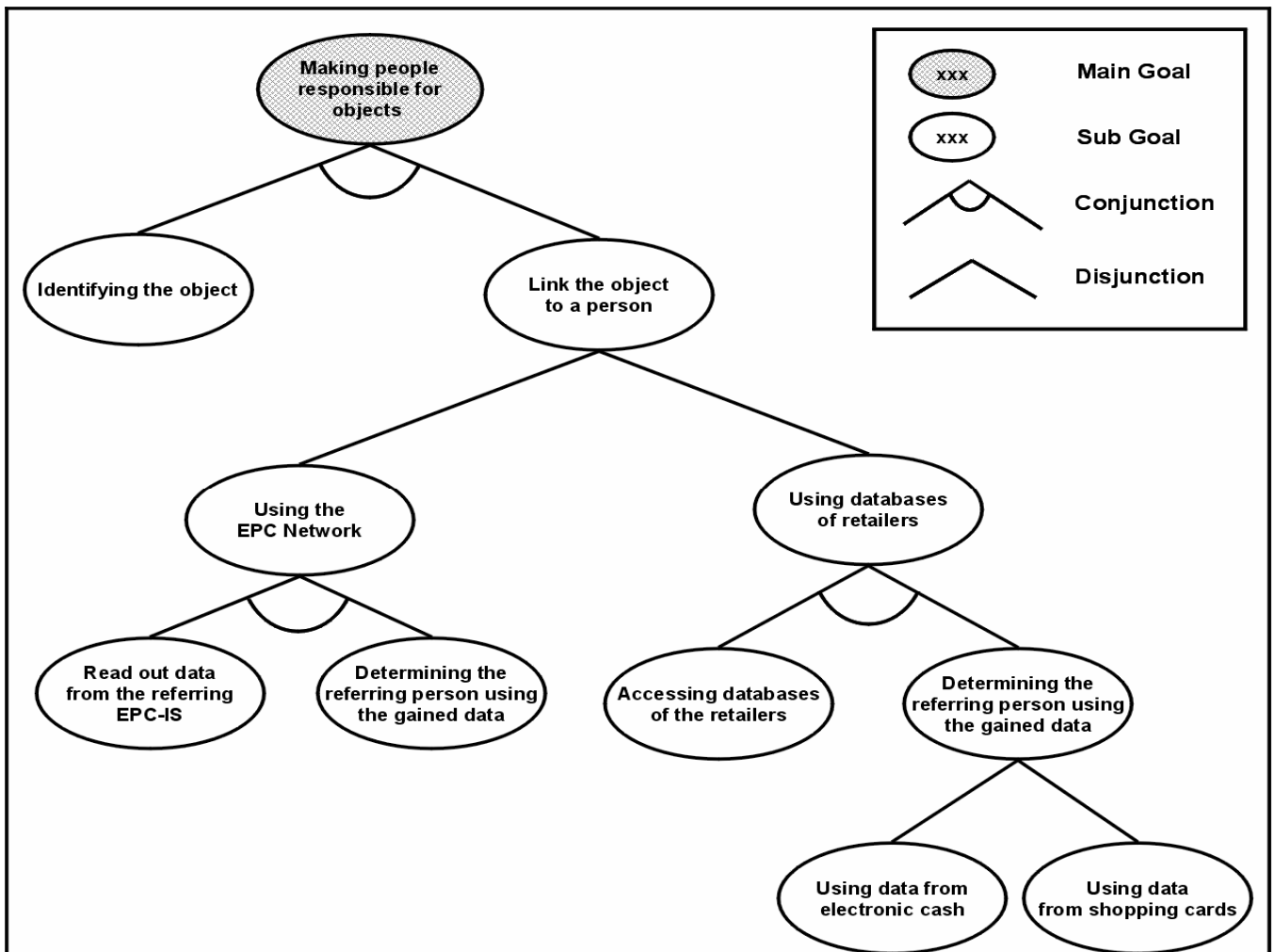
Technology Paternalism



Not anybody should be easily able to use the EPC Network to enforce rules.

- Default killing of RFID tags at store exits OR password protection of RFID tag content
- Rigorous controls and transparency of EPC Network access rights

Making people responsible for their objects



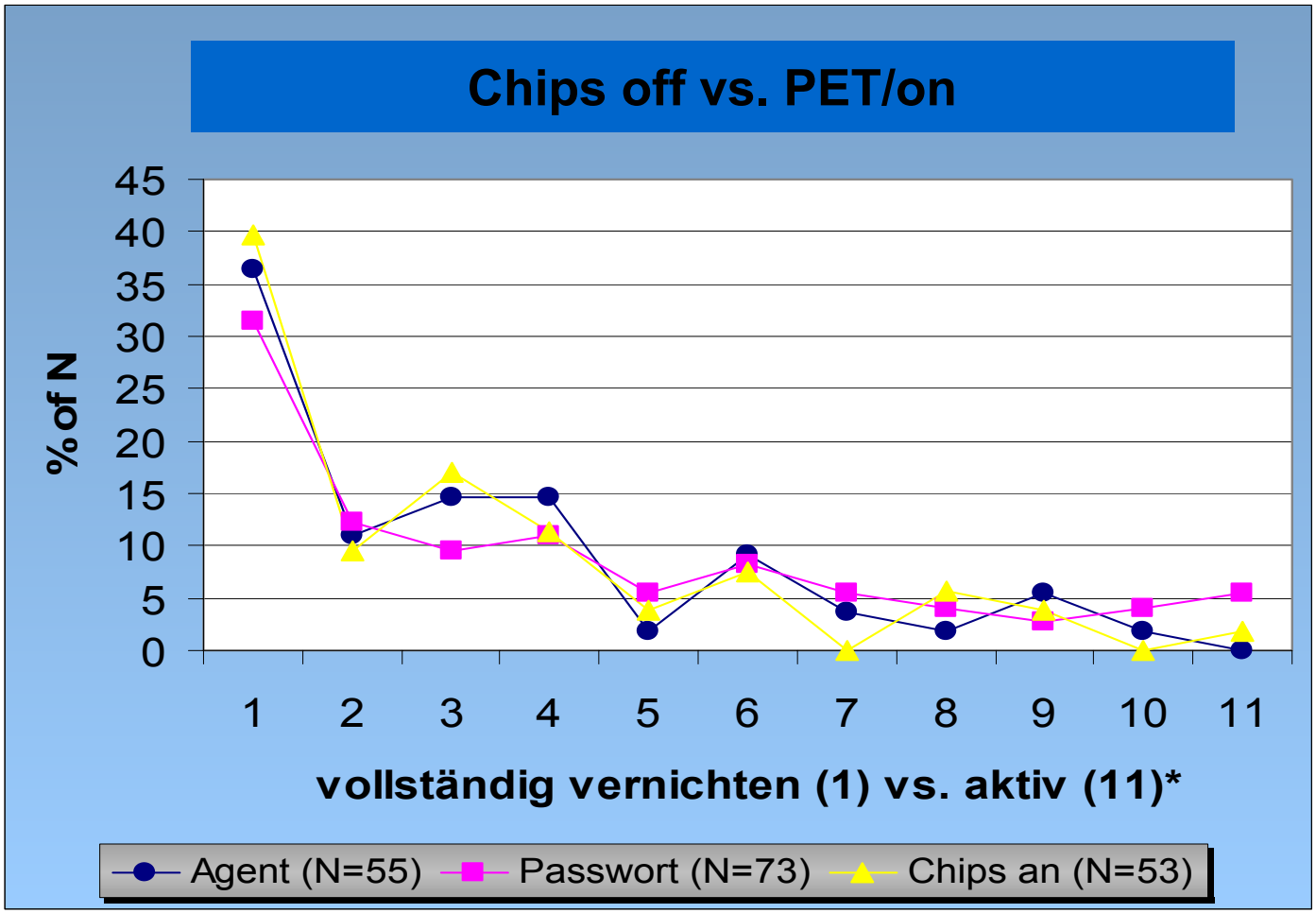
People should not be uniquely linked to their objects.

- Default killing of RFID tags at store exits OR password protection of RFID tag content
- **Partial or no saving of the full EPC serial number**
- Rigorous controls and transparency of EPC Network access rights
- **Deletion of all object data after a certain period of time**
- **Owner control over personal information on objects sold and available on the EPC Network**

A 7-Point Plan to Ensure Privacy

1. Default killing of RFID tags at store exits OR password protection of RFID tag content
2. No sharing of local tracking data (times and places) with the EPC Network beyond logistics
3. Minimal granulariy: Limited timestamp information
4. Partial or no saving of the full EPC serial number
5. Rigorous controls and transparency of EPC Network access rights
6. Deletion of all object data after a certain period of time
7. Owner control over personal information on sold objects available on the EPC Network

Default killing of RFID tags is what consumers want! 73% rather kill it, then protecting themselves with PETS!



Thank you for your attention!

For more information see:
http://interval.hu-berlin.de/content/de/projekte/technoakzept_index.php
or
contact: sspiek@wiwi.hu-berlin.de