



Forschungsinstitut für
Rationalisierung e.V.
an der RWTH Aachen

Data Security in RFID at Item Level

Tobias Rhensius

Research Institute for Operations Management (FIR) at RWTH Aachen
University

Duisburg, 12.06. – 13.06.2007

Research Institute for Operations Management (FIR) at RWTH Aachen University

We are...

- since 1953 an research institute sponsored by the state NRW at



- an research association with 145 company and federation members

- Member of



According to our view, operations management is not aimed at shedding jobs.

Rather we are striving for the improvement of a company's competitiveness and the opening-up of new markets in order to secure and create new jobs for 50 years

We have got...

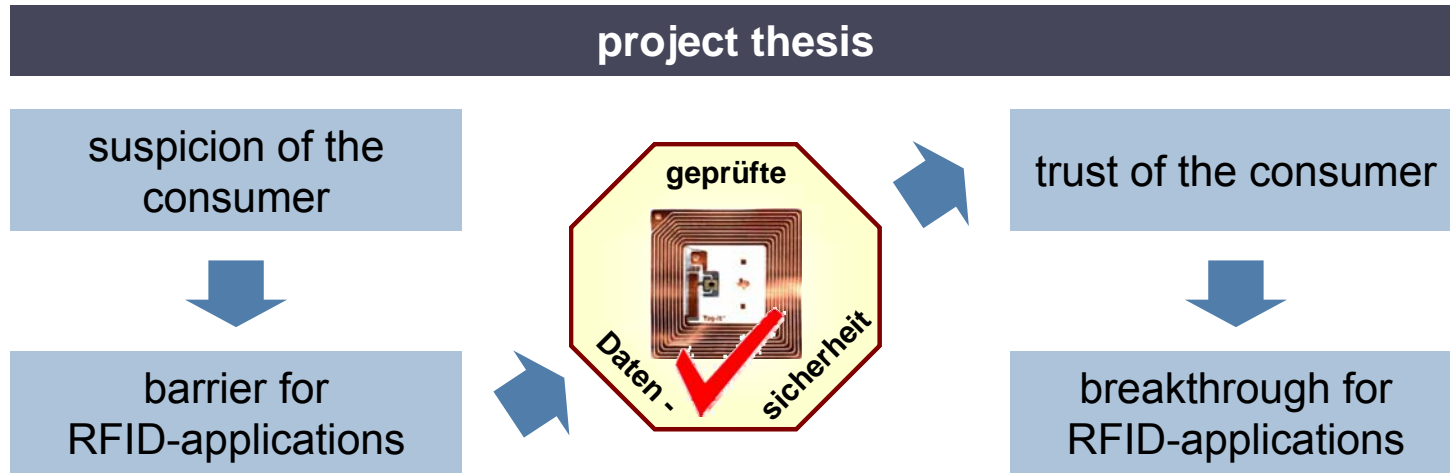
- an annual budget of about € 5 millions
- about 150 employees
- about 40 public sponsored research projects a year (sponsored by the EU, DFG, AIF, state and federal ministries)
- about 50 projects with customers of the industry and service economy per year



Thereby we are focussing on the areas:

- **information management**
- **production management**
- **service management**

Research project Trusted-RFID



intended results

- criteria catalogue for an evaluation of RFID-applications
- trust seal and process of certification
- operating concept for trust seal
- model of impact of technology-acceptance

accompanying project board



Agenda



Why data security? – Possible kinds of attacks and motives



Study about data security at item-tagging in apparel retail



Overview of safety measures



Proposal for a package of measures



Summary

Necessity of data security

abuse of the RFID-technology

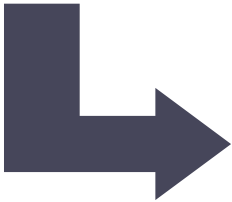
- reading out
- faking
- destroying

possible places for attacks

- Supply Chain
- Point of Sale
- After Sales

data processing

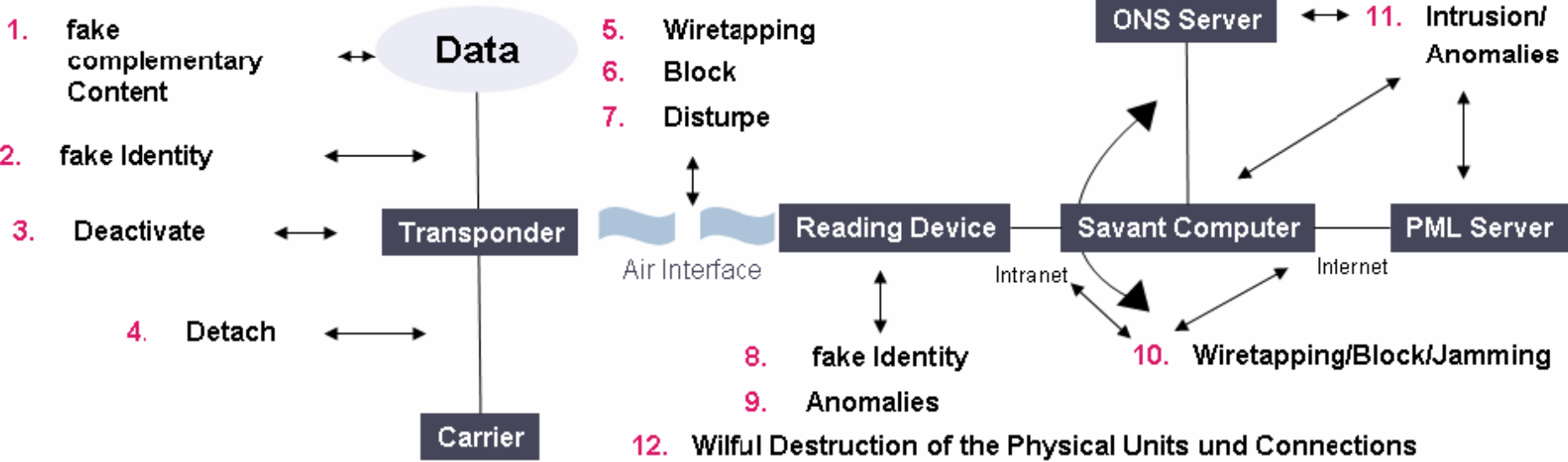
- Interaction of many components in the
 - front-end
 - back-end



guarantee of data security

- at each component
- at each communication connection
- in every process step

Possible kinds of attacks in an RFID-system

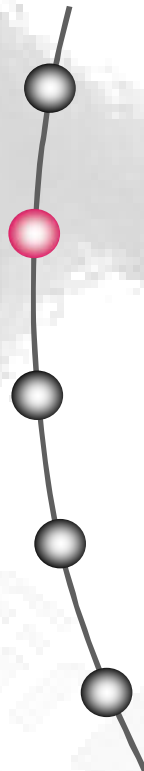


<i>committer</i>	<i>motive(s)</i>	<i>attack</i>	<i>damaged party</i>	<i>place of attack *</i>
competitor	financial motive, damnification privacy protection	1-11	system operator	SC, POS, AS
national agencies	security motive	5, 8	everybody	SC, POS, AS
system operator	financial motive	5, 8	consumer, employee	POS
cyber terrorists	damnification, profiling, fun	1-11	system operator (everybody)	SC, POS, AS
employee	security (anonymity), cheat	1-7	system operator; (national agencies)	SC, AS
consumer	cheat, security (anonymity)	1-7	system operator; (national agencies)	SC, AS

* SC = Supply Chain POS = Point of Sale AS = After Sales



Agenda

- 
- Why data security? – Possible kinds of attacks and motives
 - Study about data security at item-tagging in apparel retail**
 - Overview of safety measures
 - Proposal for a package of measures
 - Summary

Study: „Data Security at Item-Tagging in Apparel retail“

Objects of the study

- goals of the RFID-application
- technical requirements
- safety measures
- cost aspects

Participants

- 23 medium – big size german apparel retailer
- sector: IT and logistics
- position: mainly chief executives or manager



photocase.de

A Persönliche und betriebliche Informationen

1. Name/Funktion im Unternehmen: _____
 2. Bei Geschäftstätigkeit: Privatsphäre / Geschäftszweck
 3. Umgang mit Unternehmensdaten: als Kunde / als Mitarbeiter

C Ziele des RFID-Einsatzes

1. Wie wichtig sind Ihnen die folgenden Ziele beim RFID-Einsatz? (Bewerten Sie diese bitte in einer Rangfolge von "1" bis "7" (sehr wichtig bis gar nicht wichtig)).

1. Erhöhung der Prozessqualität
 2. Reduzierung der Kosten
 3. Erhöhung der Transparenz
 4. Erhöhung der Flexibilität
 5. Erhöhung der Sicherheit
 6. Erhöhung der Kundenzufriedenheit
 7. Erhöhung der Effizienz

1. Sollten RFID-Tags auf einzelnen Artikeln im Einzelhandel zulassen, die relevanten Produktinformationen (z.B. mit dem Etikettensystem) zu lesen? (Bitte wählen Sie die für Sie zutreffende Antwort aus.)
 Ja, wenn keine weiteren Daten
 Ja, wenn weitere Daten (z.B. Lieferant, Preis, etc.)
 Ja, wenn weitere Daten (z.B. Preis, Lieferant, etc.)
 Ja, wenn weitere Daten (z.B. Preis, Lieferant, etc.)
 Ja, wenn weitere Daten (z.B. Preis, Lieferant, etc.)

F Kosten

1. Wie hoch ist der Aufwand für die Einführung von RFID-Tags? (Bitte bewerten Sie dies in einer Rangfolge von "1" bis "7" (sehr wichtig bis gar nicht wichtig)).

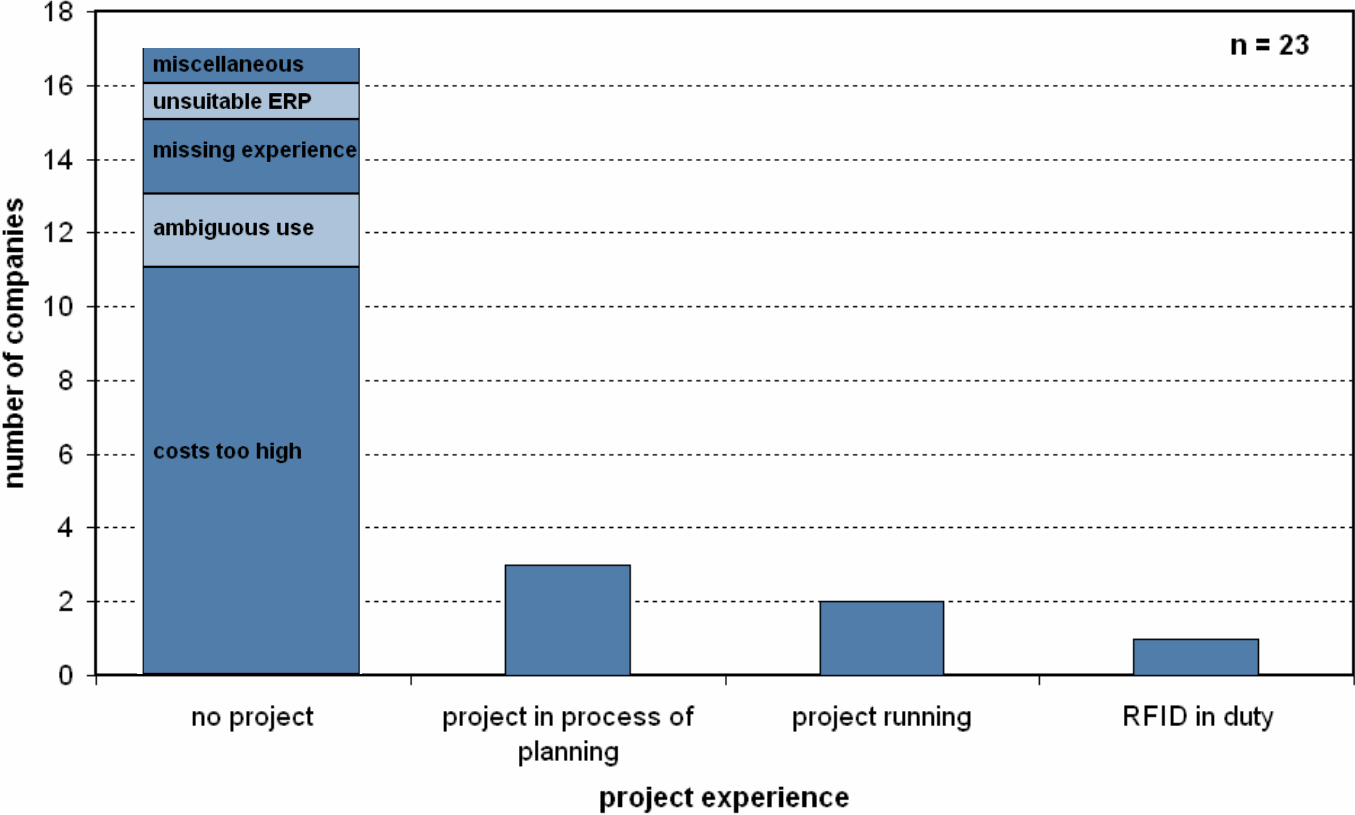
1. Hohe Anfangsinvestition
 2. Hohe laufende Kosten
 3. Hohe Wartungskosten
 4. Hohe Schulungskosten
 5. Hohe Kosten für die Integration in bestehende Systeme
 6. Hohe Kosten für die Integration in bestehende Systeme
 7. Hohe Kosten für die Integration in bestehende Systeme

G Verschiedenes

1. Durch welche Maßnahmen können die Datenschutzrisiken bei der RFID-Einführung am besten reduziert werden?
 durch keine Maßnahmen
 durch technische Maßnahmen
 durch organisatorische Maßnahmen
 durch rechtliche Maßnahmen
 durch technische, organisatorische und rechtliche Maßnahmen



Results of the study (1): project experience with RFID

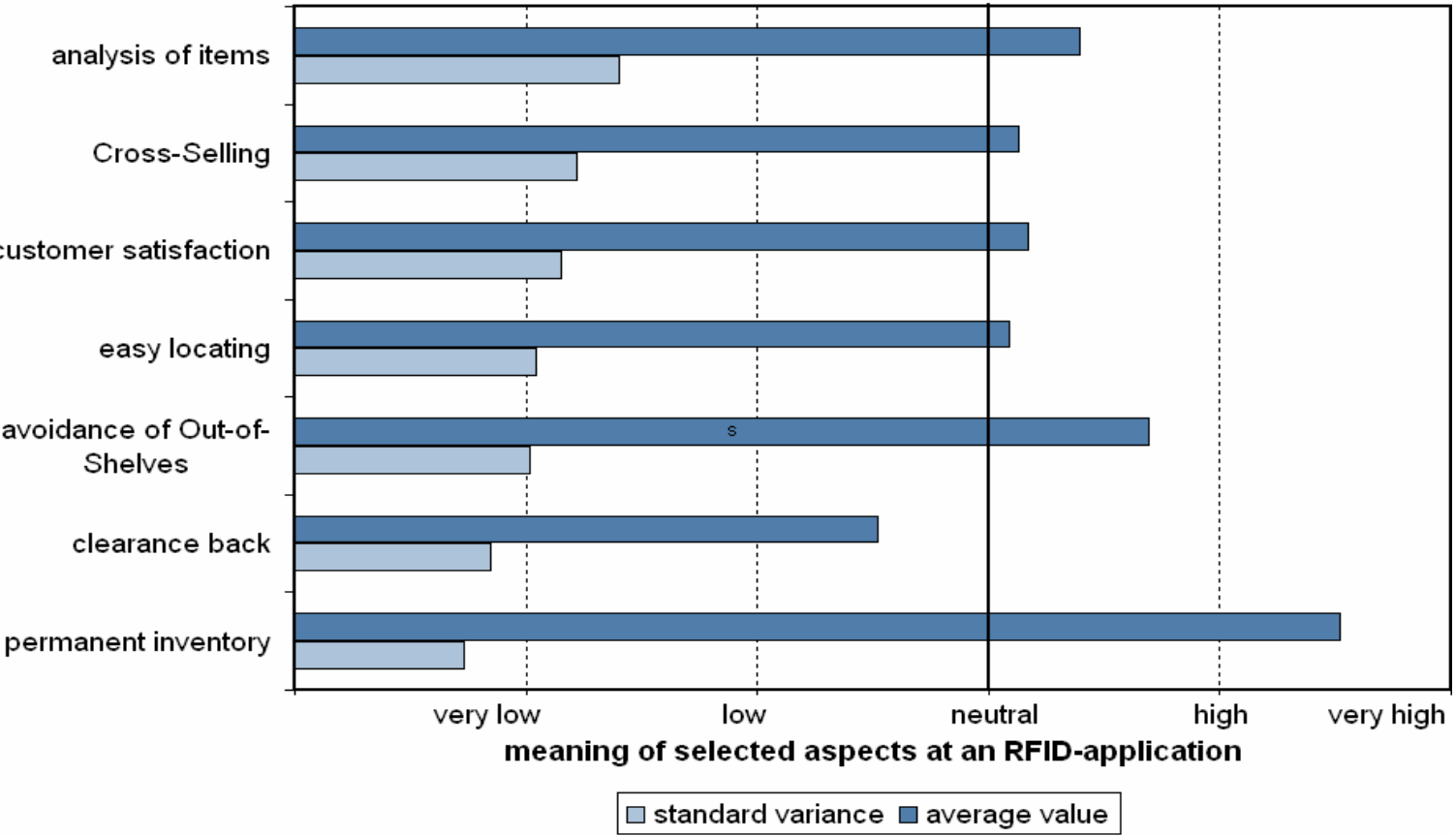


78 % of the companies know RFID, only 26 % made experiences in projects

Main reason against a pilot project: costs too high



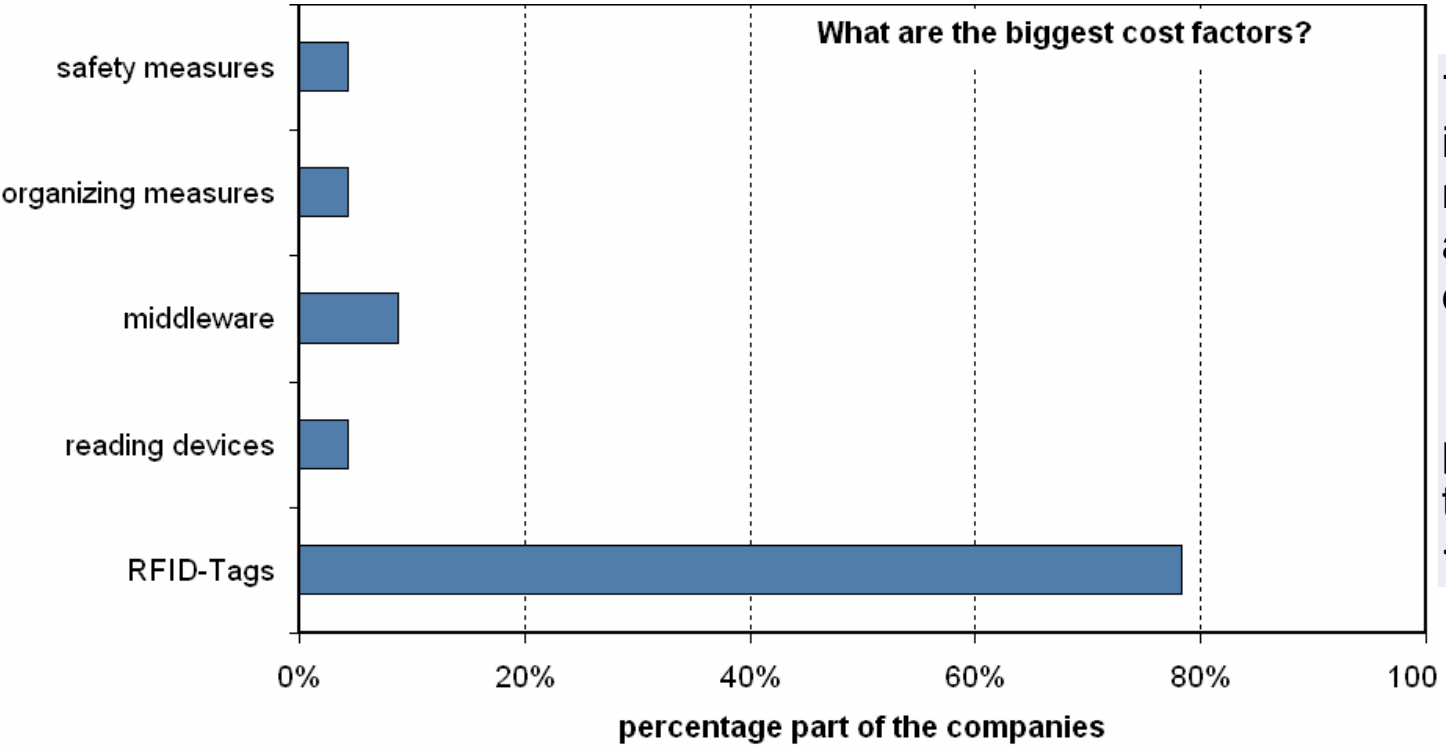
Results of the study (2): goals of the RFID-application



goal of the RFID-application: increase in efficiency and process quality

most important aspects: permanent inventory, avoidance of Out-of-Shelves situations

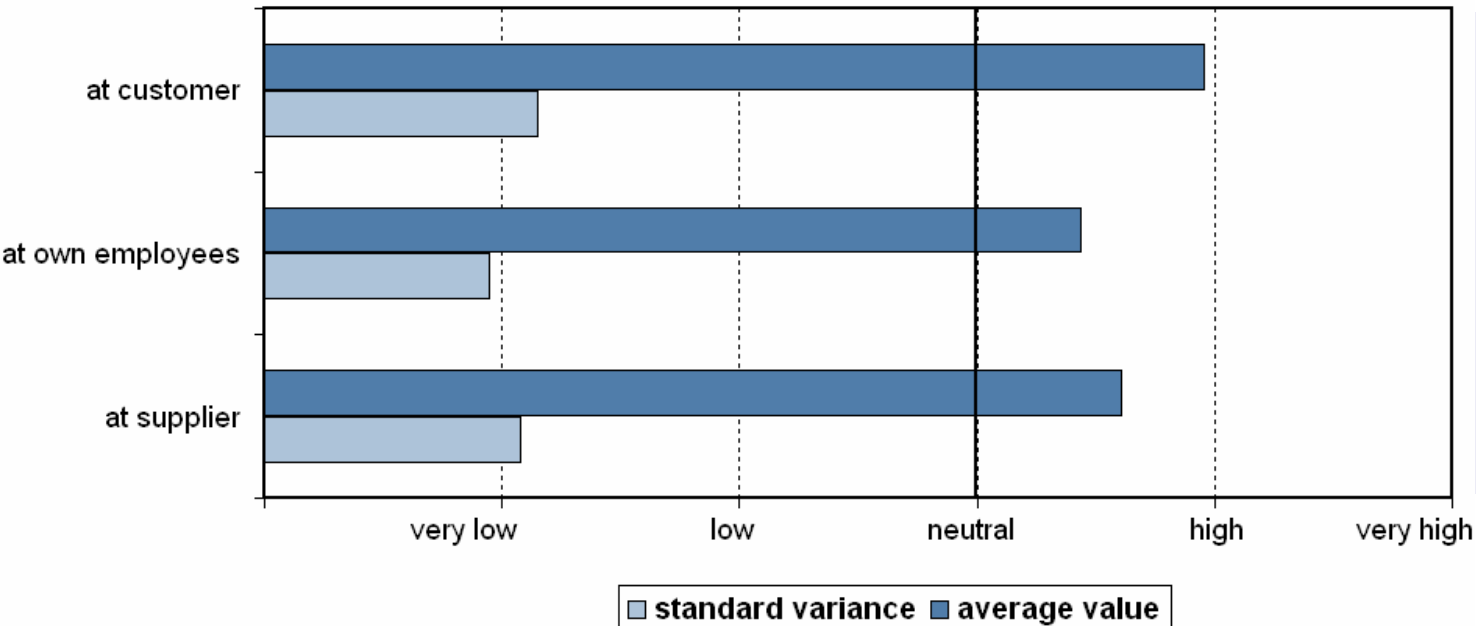
Results of the study (3): meaning of the cost factors



78 % of the interviewed persons regard RFID-Tags as the biggest cost driver

► claim: piece price for the transponder < 5 Cent

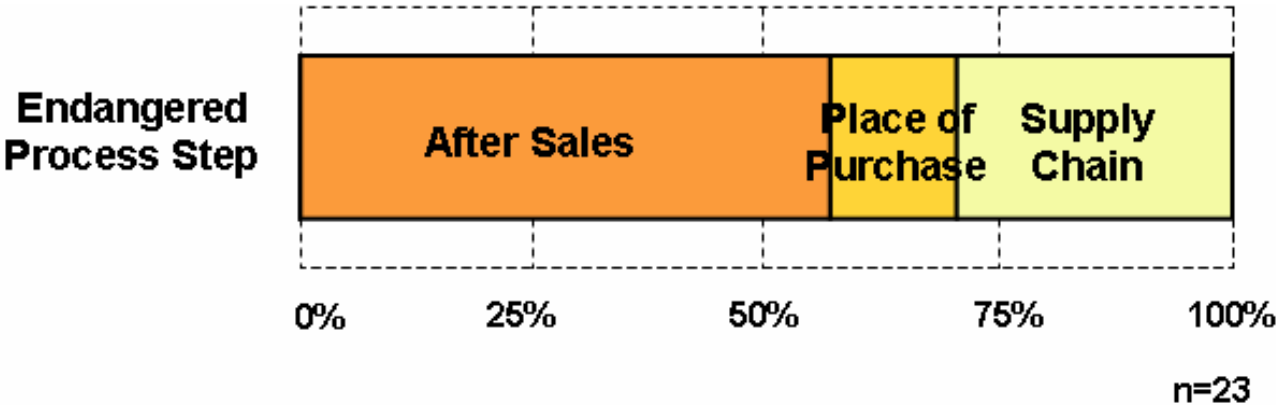
Results of the study (4): meaning of data security for the acceptance of RFID



high meaning of data security for acceptance at customer and supplier

only slight positive evaluation at own employees

Results of the study (5): endangered process steps



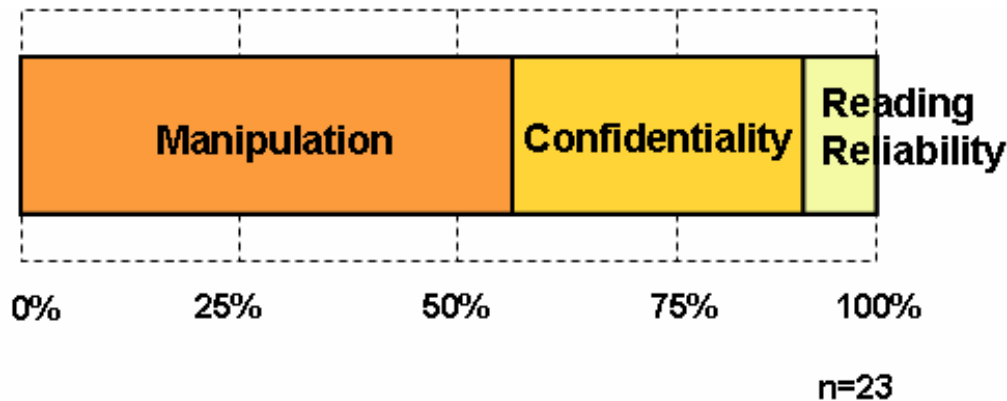
for 57 % the After Sales represents the greatest risk for data security

30 % regard the Supply Chain as most endangered

Source: Research Institute for Operations Management (2006)

Results of the study (6): dangers in the After Sales

**Dangers
(in the
After
Sales)**



Source: Research Institute for Operations Management (2006)

outstanding necessary safety measures:

in the Supply Chain

- ▶ against the violation of data confidentiality (48%)

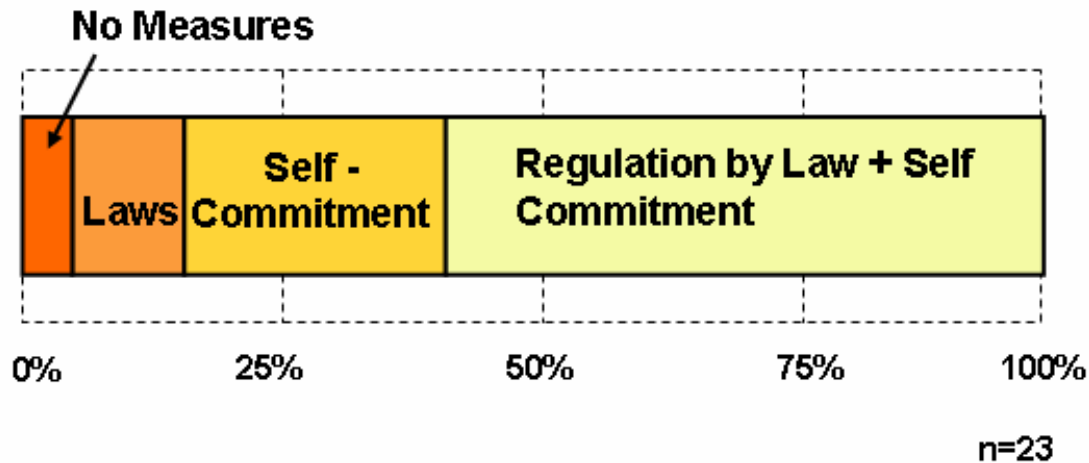
in the Point of Sale

- ▶ against data manipulation (61%)

in the After Sales

- ▶ against data manipulation (57%)

Results of the study (7): measures to guarantee data security



87 % of the apparel retailers want to assure the data security by a self-commitment (exclusive / parity with laws)

Source: Research Institute for Operations Management (2006)

Agenda

- Why data security? – Possible kinds of attacks and motives
- Study about data security at item-tagging in apparel retail
- Overview of safety measures**
- Proposal for a package of measures
- Summary

Safety measures (1/4)

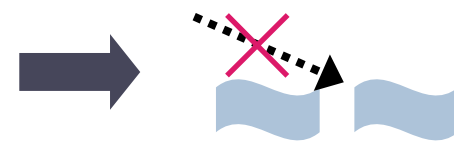
A Authentication

- prevention of attacks
 - where the data content will be faked
 - which aim at the reading devices
- takes place before the proper data transfer
- check, whether the components (tags + reading devices) belong to the same application
- without additional safety measures:
 - ▶ attack on the air interface possible



B Encryption

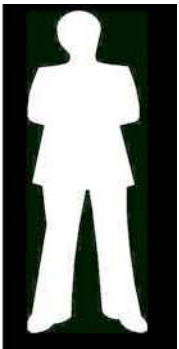
- aims at the protection of the air interface
- prevention of illegal eavesdropping
- recording a personal file is still possible, but appreciably more difficult
- heavy modification of the data by the algorithm
 - ▶ insight into the real content will be prohibited
- critical: management and communication of the keys



Safety measures (2/4)

C MetaID

- aims at the protection of the transponder data & air interface
- transponder gets an new identity (complementary / substituting)
- possible kinds of attacks without additional safety measures
 - „reply-attacks“
 - deleting the contents in rewriteable transponders



D Deactivation

- aims at the anonymity of the transponder
- temporary or permanent deactivation possible
- critical: obtaining of the whole potential of RFID-technology (esp. In the After-Sales) not possible anymore



Safety measures (3/4)

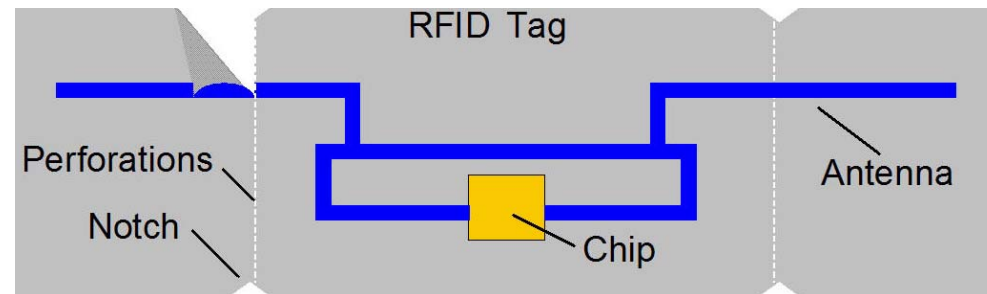
E Data integrity

- aims at the protection of the communication of the air interface
- measures enable faultless and complete transfer of data via the air interface



F Physic procedures

- contains all the procedures, which are associated with additional physical effort, e. g. :
 - screening
 - curtail the radio radius



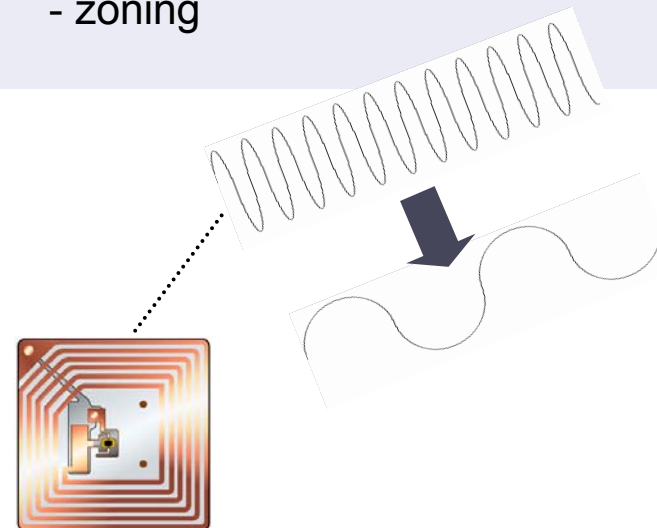
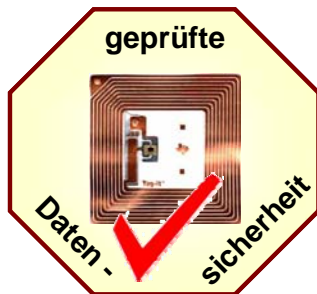
Safety measures (4/4)

G Self-commitment

- commitment of compliance with security
 - towards consumer
 - towards competitor
- base
 - guidelines, principles, mission statements
 or
 - certification with a trust sign

H Miscellaneous

- further safety measures, which aren't assignable to any of the other groups
- e.g.:
- detection of double EPC-numbers
 - analysis of the antenna energy
 - alternation of the radio frequency
 - zoning



Agenda

- Why data security? – Possible kinds of attacks and motives
- Study about data security at item-tagging in apparel retail
- Overview of safety measures
- **Proposal for a package of measures**
- Summary

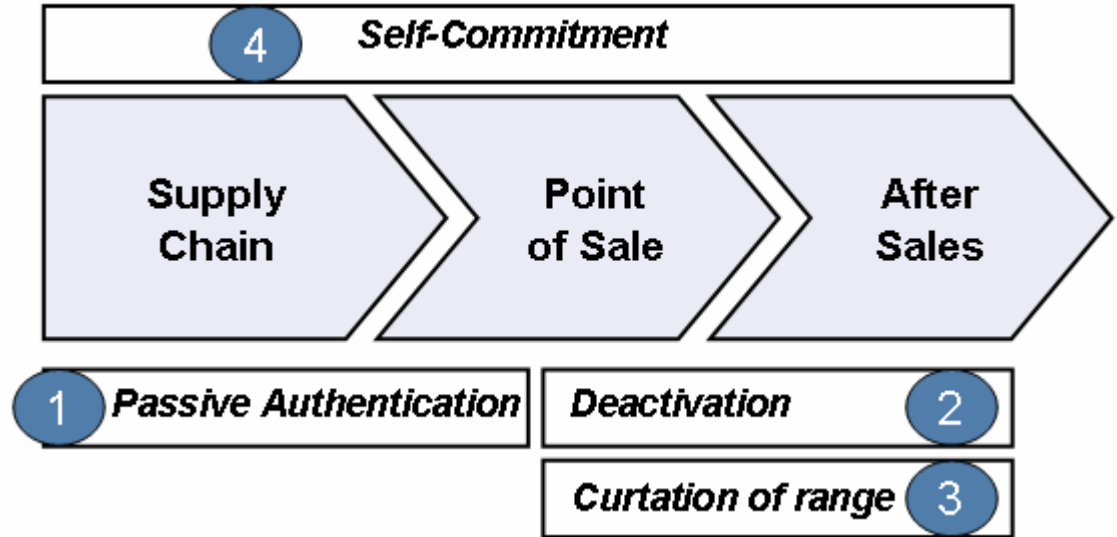
Package of measures 4PPS (1/4)

exclusive implementing of measures A – H has got critical disadvantages:

- too complex (B encryption – Chained-Hash-Lock-operation)
- too intricately (F physical procedures – blocker-tags)
- not advisable (D deactivation – kill-function / permanent deactivation)
- not sufficient (G self-commitement – compliance of principles)



development of 4PPS
= „For Puplic Privacy and Security“
= „4-Point-Package-for-Security“



Package of measures 4PPS (2/4)

M1: Authentication

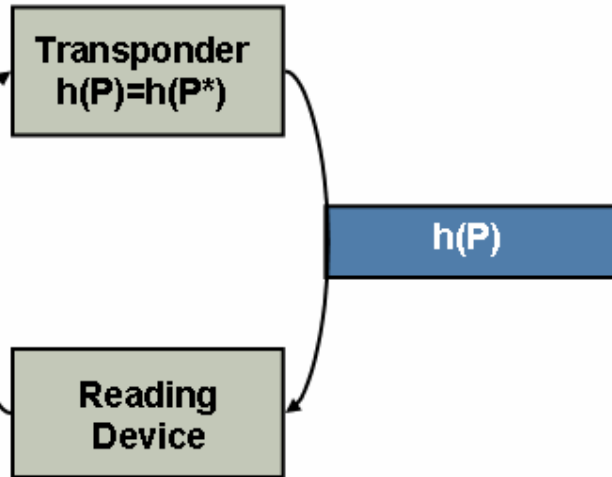
4 Alternatives:

$h(\text{EPC}; h(\text{P}))$

$h(\text{EPC}; \text{TagID})$

$\text{XOR}(\text{EPC}; h(\text{P}))$

$\text{XOR}(\text{EPC}; \text{TagID})$



- aims at the protection of Point of Sale & Supply Chain

M2: Temporary deactivation

- claims of the apparel retailer: temporary deactivation of the transponders without an active demand of the customer
- alternative 1: access key used for authentication can be overwritten with a new one & handed over to the customer
- alternative 2: encryption of the serial number of the EPC
- ▶ quasi deactivation
- customer demand: kill-function

Package of measures 4PPS (3/4)

M3: Change of the reading range

- detaching of the antenna
Effect: transponder will only report if the reading device is very close to it, otherwise not
- advantage: transponder data remains in the memory
- ▶ goal: application together with measure point 2
- positive effect onto the uncertainty of the customer

M4: Self commitment

- connection of all process steps to self committing measures!
- Point of Sale: signs to point out
 - the impossible manipulability of the transponder data
 - the guarantee of anonymity
- special signposts at the checkout
- holistic compliance with principles by a certificate
- ▶ confidence of the consumer will be strengthened

Package of measures 4PPS (4/4): upshot

What is 4PPS able to?

- illegal eavesdropping of the air interface will be prohibited
- detection of plagiarism by reply-attacks according to the EPC-procedure
- persecution, tracking in Supply Chain & After Sales warded off
- impossible to overwrite & delete the transponder data
- surveillance of the consumer in the After Sales will be prohibited
- unauthorised using of customer data on the transponders can be avoided

What isn't 4PPS able to?

in Supply Chain & at Point of Sale:

- prohibition of blocking & jamming
- avoiding of destroying & detachment of the transponder

but...

in all process steps:

- Destroying & detachment of the transponder can be averted by integration

in the After Sales:

- blocking and jamming can be prohibited by deactivation or detachment of the antenna



claims completely fulfilled !!!

Agenda

Why data security? – Possible kinds of attacks and motives

Study about data security at item-tagging in apparel retail

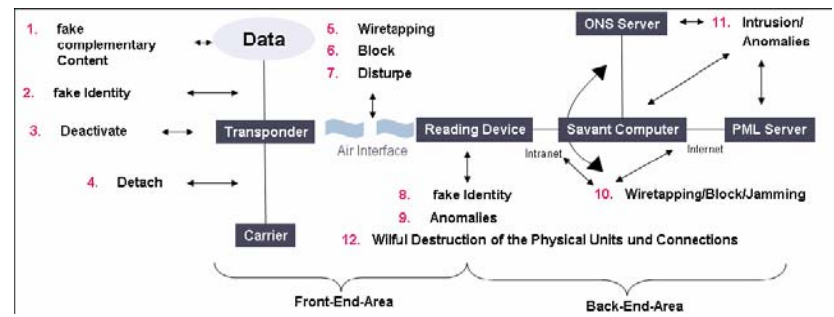
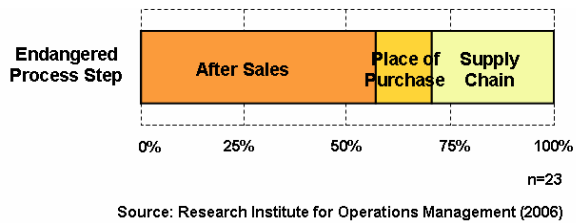
Overview of safety measures

Proposal for a package of measures

Summary

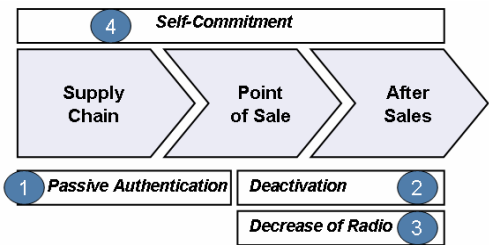
Summary

1. Why data security? – Possible kinds of attacks and motives



2. Study about data security at item-tagging in apparel retail

3. Overview of the safety measures



4. Proposal for a package of measures

www.fir.de



Research Institute for
Operations Management at
RWTH Aachen University

Pontdriesch 14/16
52062 Aachen
www.fir.rwth-aachen.de

Dipl.-Wirt.-Ing.

Tobias Rhensius MSc

Bereich Informationsmanagement

Telefon: +49 (0)241 477 05-510

Fax: +49 (0)241 477 05-199

Mobil: +49 163 841 23 76

Email: Tobias.Rhensius@fir.rwth-aachen.de

Thank you for your attention