



Seminararbeit RFID und Privatheit

Christoph Balling

Seminararbeit betreut von Dipl.-Inform. Mirco Stern



12.06.06

- (1) Einleitung
- (2) Informationelle Selbstbestimmung
- (3) RFID Technologie
- (4) Gefahren beim Einsatz der RFID Technologie
- (5) Möglichkeiten die Privatheit herzustellen
- (6) Zusammenfassung
- (7) Diskussion

(1) Einleitung

(2) Informationelle Selbstbestimmung

(3) RFID Technologie

(4) Gefahren beim Einsatz der RFID Technologie

(5) Möglichkeiten die Privatheit herzustellen

(6) Zusammenfassung

(7) Diskussion

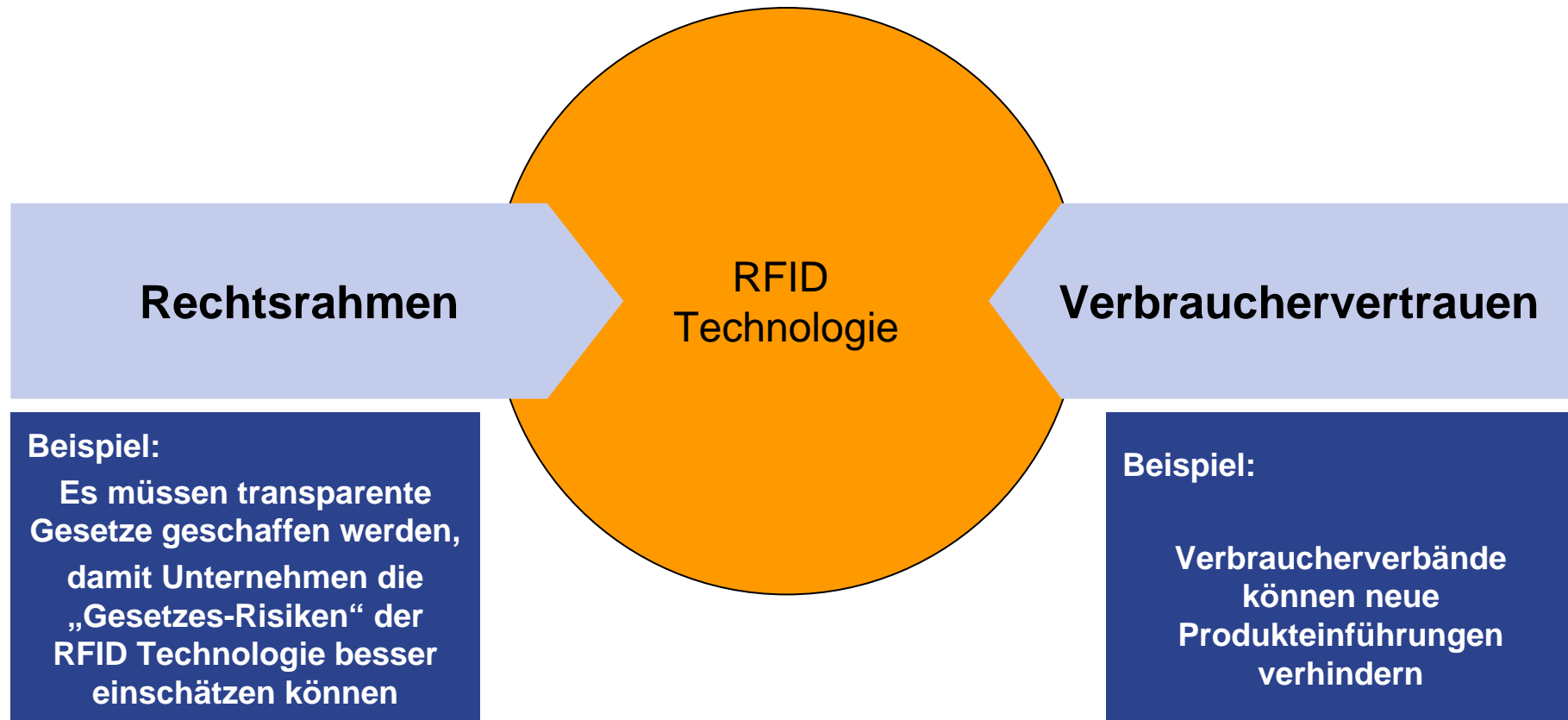
Radio Frequency Identification ein wichtiger Baustein für eine allgegenwärtige Datenverarbeitung

**Radio Frequency Identification (RFID)
als Schlüsseltechnologie
für eine allgegenwärtige Datenverarbeitung**

„Soll die allgegenwärtige Rechnertechnik **gerade im Hintergrund** und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen, kann sie nicht zugleich dem Betroffenen **bewusst gegenwärtig** sein.“

Alexander Roßnagel, 2005

Der Erfolg der RFID Technologie hängt von mehreren Faktoren ab



- (1) Einleitung
- (2) Informationelle Selbstbestimmung**
- (3) RFID Technologie
- (4) Gefahren beim Einsatz der RFID Technologie
- (5) Möglichkeiten die Privatheit herzustellen
- (6) Zusammenfassung
- (7) Diskussion

Europäischen Charta der Grundrechte (7.12.2000)

Artikel 8 [Schutz personenbezogener Daten]

(1) Jede Person hat das Recht auf Schutz der sie betreffenden Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden.

Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

...

Das Datenschutzrecht erwartet vom Unternehmen den Verbraucher über die Datenverarbeitung zu informieren

bereits auf dem Produkt
und an den Verkaufsregalen

Das Datenschutzrecht verpflichtet Unternehmen Verbraucher zu informieren, wenn über RFID Chips personenbezogene Daten verarbeitet werden.

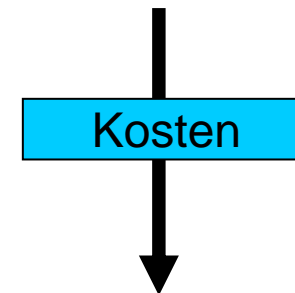
erhoben, gespeichert,
verwendet oder weitergegeben

gemäß § 3 Absatz 1
Bundesdatenschutzgesetz:
„Einzelangaben über persönliche
oder sachliche Verhältnisse einer
bestimmten oder bestimmbaren
natürlichen Person“

- (1) Einleitung
- (2) Informationelle Selbstbestimmung
- (3) RFID Technologie**
- (4) Gefahren beim Einsatz der RFID Technologie
- (5) Möglichkeiten die Privatheit herzustellen
- (6) Zusammenfassung
- (7) Diskussion

Je nach Anwendung sollte man den richtigen Tag wählen

Art des Tag	maximale Reichweite
passiv	7 Meter
semiaktiv	15 Meter
aktiv	100 Meter



längere Reichweiten nicht immer sinnvoller
(Beispiel: Zuordnung des Skipass)

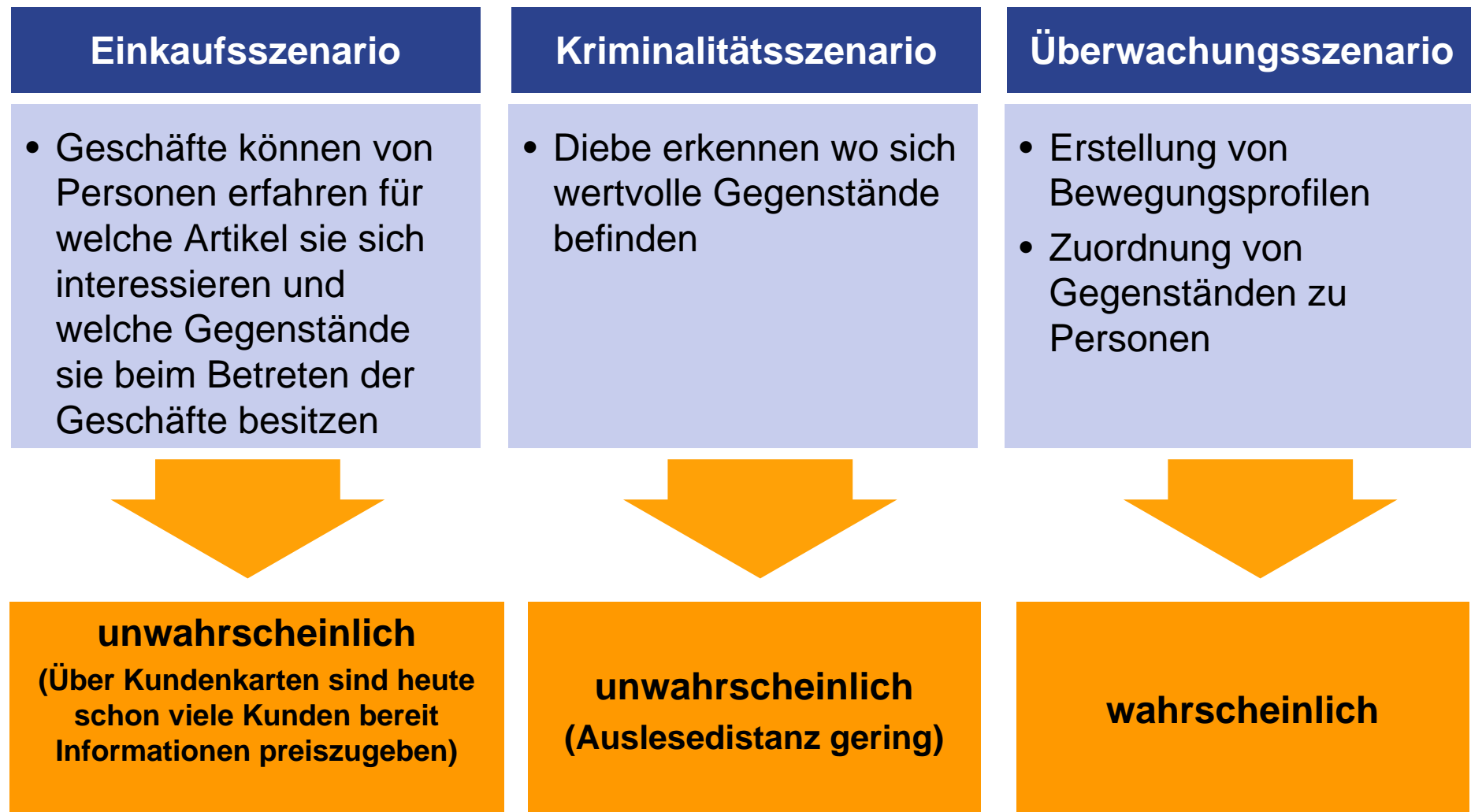
Einige Vorteile der RFID Technologie im Überblick

Vorteil	Anwendungsbeispiel
Authentifikation	Banknoten
Individuelles eingehen auf Personen	schnelles Behandeln von Risikopatienten
Reduzierung von Menschen verursachter Fehler	Werkzeugmanagement in der Flugzeugwartung (richtiges Werkzeug verwenden; an richtige Stelle nach Nutzung legen)
Erhöhung der Prozessgeschwindigkeit	Bibliothek (einfachere Inventur; Vorsortierung bei Buchrückgabe)

- (1) Einleitung
- (2) Informationelle Selbstbestimmung
- (3) RFID Technologie
- (4) Gefahren beim Einsatz der RFID Technologie**
- (5) Möglichkeiten die Privatheit herzustellen
- (6) Zusammenfassung
- (7) Diskussion

Viele Bürger haben Ängste vor der RFID Technologie

Nach Marc Langheinrich entwickelte Szenarien der Kundenangst:



Die Gefahren der RFID Technologie werden unterschiedlich wahrgenommen

- RFID ein weiterer Schritt zur Orwellschen Gesellschaft?
 - fehlende Erkenn- und Rekonstruierbarkeit der Datenerhebung
 - könnte Gegenstände einer Person zuordnen
 - ⇒ Tracking von Personen wird leichter möglich
 - ⇒ Soziale Netzwerke werden erkennbar

Eine Gefahrenklassifikation von Sarah Spiekermann

- **Konsumentenbedenken nach Sarah Spiekermann**
 - 1) **Unbemerktetes Auslesen – Kontrollverlust im engeren Sinne**
(Benutzer weiß überhaupt nicht, dass seine Informationen preisgegeben werden)
 - 2) **Verfolgbarkeit**
(Es können Bewegungsprofile des Benutzers erstellt werden)
 - 3) **Objektverantwortlichkeit**
(Zurückführbarkeit des Objekts auf Benutzer)
 - 4) **Technologiepaternalismus**
(Technologie schränkt die Handlungsmöglichkeit des Benutzers ein;
Beispiel: Wenn man sich nicht anschnallt ertönt ein Warnsignal)
 - 5) **Personalisierung mit negativen Konsequenzen**
(Personen werden eingeordnet und wieder erkannt)
 - 6) **Krimineller Missbrauch**
(Dritte könnten privaten Besitz auslesen)

- (1) Einleitung
- (2) Informationelle Selbstbestimmung
- (3) RFID Technologie
- (4) Gefahren beim Einsatz der RFID Technologie
- (5) Möglichkeiten die Privatheit herzustellen**
- (6) Zusammenfassung
- (7) Diskussion

Primär durch technische Mittel sollte man die Privatheit herstellen

- Privatheit herstellbar

- durch technische Mittel

- durch soziale Mittel
(Leitlinien von Unternehmen)
- durch rechtliche Mittel
(Bundesdatenschutzgesetz)

PET
(Privacy-enhancing technologies)

„Was technisch verhindert wird, muss nicht mehr verboten werden.“

Alexander Roßnagel, 2005

Auf dem ersten Blick die einfachste Variante Privatheit herzustellen

Killer Tag

Der Tag wird unlesbar gemacht

- Zeitaufwand
- Verbraucher kann nur schwer überprüfen ob Tag auch wirklich zerstört ist
- nach Verkauf des Artikels könnte RFID für Verbraucher noch nützlich sein

Der Verbraucher will selbst die Kontrolle haben

“Clipped Tag“ Verfahren

Verbraucher kann Antenne des RFID-Chips zerstören,
was zur starken Reduzierung der Übertragungsdistanz führt

- + für Verbraucher kontrollierbar
- + einfach durchzuführen
- + könnte mit Zusatzantenne wieder reaktiviert werden

- bei geringen Reichweiten noch auslesen möglich

Ein Verfahren welches für andere Anwendungen zu Problemen führen kann

Blocker Tag

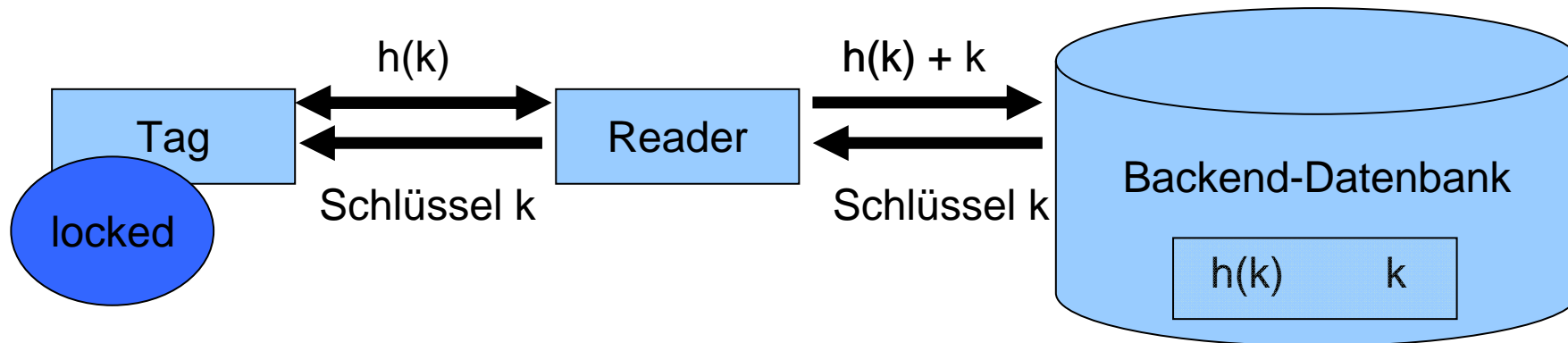
Der Tag gibt dem Leser vor es wären 2^{64} Tags in seinem Lesebereich
Für Lesegerät wird es so gut wie unmöglich „echte“ Tags auszulesen

+ kostengünstig

- durch bessere Lesegeräte können Blocker Tags ignoriert werden (z.B. Triangulation, Signalstärke) und Lesegerät kann somit normale RFID Tags auslesen
- könnte ungewollt andere Leser stören

MetaIDs ermöglichen keinen direkten Zugriff

Hash-Locks Verfahren



- + einfach zu implementieren
- Tracking noch möglich
- benötigt vernetzte Datenbank

Randomized Hash-Locks ermöglichen kein Tracking mehr

„Randomized Hash-Locks“

Hier sendet der Tag $h_T(ID || r)$ und Zufallszahl r .
Leser benötigt komplette Liste aller ID's.
Leser bildet mit allen ID's Hash bis gleich $h_L(ID || r)$.

- + Tracking nicht mehr so einfach möglich
- + günstiger als aufwendige kryptographische Verfahren
- Skalierbarkeit bei vielen Tags problematisch
- keine kryptographische Robustheit
- wenn einmal die ID offen gelegt wird, ist im nachhinein Tracking möglich

Eine Übersicht welche Verfahren welche Risiken einschränken

	Unbemerkt Auslesen	Verfolgbarkeit	Objektverant- wortlichkeit	Technologie- paternalismus	Personalisierung	Krimineller Missbrauch
Killer Tag	++	++	++	++	++	++
Clipped Tag	+	++	-	++	++	++
Blocker Tag	-	-	-	-	-	-
Hash Locks	++	-	+	+	+	++
Randomized Hash Locks	++	+	+	++	++	++

wird verhindert (++)

wird eingeschränkt (+)

wird nicht verhindert (-)

Das Datenschutzaudit ist ein wichtiges Instrument, damit die technischen Verfahren auch dem Verbraucher glaubwürdig erscheinen

Datenschutzaudit

- Datenschutzkonzept wird extern überprüft
- Selbstregulierung
- Datenschutzfreundliche Technikgestaltung wird vorangetrieben
- Wettbewerb um den besseren Datenschutz
- schafft Vertrauen beim Kunden



Agenda

- (1) Einleitung
- (2) Informationelle Selbstbestimmung
- (3) RFID Technologie
- (4) Gefahren beim Einsatz der RFID Technologie
- (5) Möglichkeiten die Privatheit herzustellen
- (6) Zusammenfassung**
- (7) Diskussion

Zusammenfassung

- Abwägung zwischen Handhabbarkeit und Privatheit ist notwendig.
- Risiken komplett einzuschränken ist kaum möglich.
- Um die Akzeptanz zum Kunden zu erhöhen, größtmögliche Transparenz und Konsumentenaufklärung beim Einsatz der RFID Technologie.

Agenda

- (1) Einleitung
- (2) Informationelle Selbstbestimmung
- (3) RFID Technologie
- (4) Gefahren beim Einsatz der RFID Technologie
- (5) Möglichkeiten die Privatheit herzustellen
- (6) Zusammenfassung
- (7) Diskussion**

Anhang

Grundgesetz

Artikel 1

[Menschenwürde; Grundrechtsbindung der staatlichen Gewalt]

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

...

Artikel 2

[Allgemeine Handlungsfreiheit; Freiheit der Person; Recht auf Leben]

...

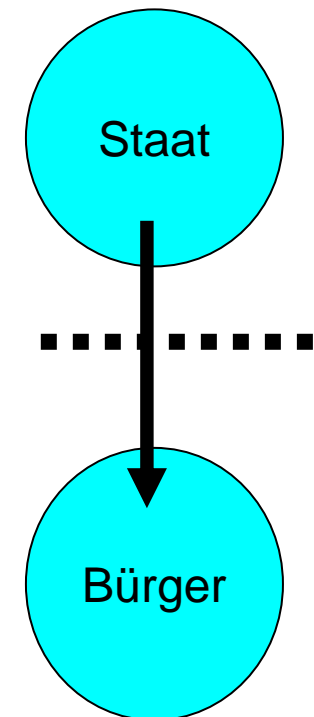
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. ...

Auszug Volkszählungsurteil Bundesverfassungsgericht (1983)

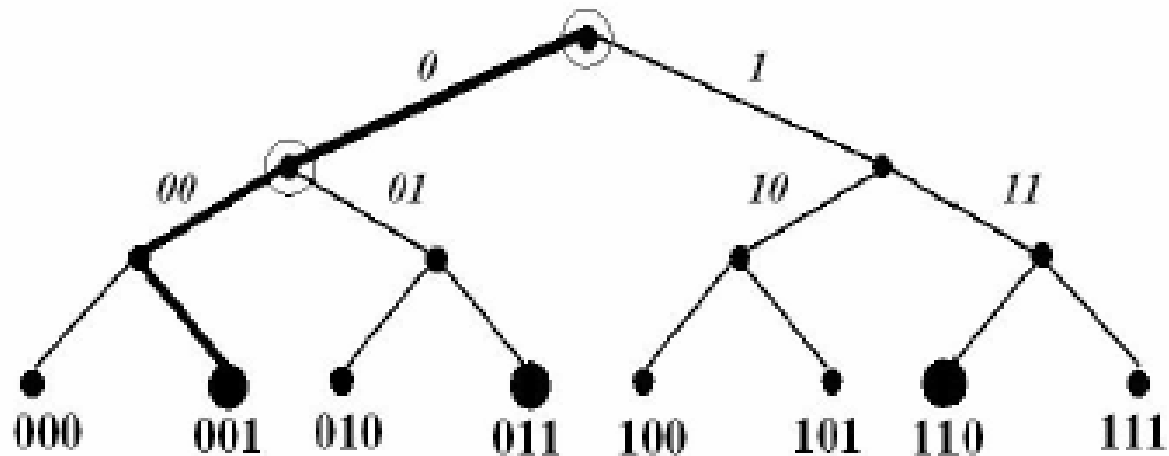
keine schrankenlose Gewährleistung des
Artikel 2 I in Verbindung mit Art.1 I Grundgesetz

...

Grundsätzlich muss daher der Einzelne Einschränkungen seines
Rechts auf informationelle Selbstbestimmung *im überwiegenden
Allgemeininteresse hinnehmen*.



Beim „Tree-Walking Singulation“ Protokoll und einfachen Lesern würde der Blocker Tag funktionieren



folgende Tags sind im Lesebereich:

- 1: 001**
- 2: 011**
- 3: 110**

Die allgegenwärtige Datenverarbeitung steht im Konflikt mit der Kontrolle der eigenen Daten

„The problem, while often couched in terms of privacy, is really one of control. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, where information is flowing, how it is being used, what is broken, and what are the consequences of any given action.”

Mark Weiser, 1991

„Soll die allgegenwärtige Rechnertechnik **gerade im Hintergrund** und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen, kann sie nicht zugleich dem Betroffenen **bewusst gegenwärtig** sein.”

Alexander Roßnagel, 2005

Literatur

- [1] Marc Langheinrich: RFID and Privacy. In: Milan Petkovic; Willem Jonker (Eds.): Security, Privacy, and Trust in Modern Data Management; Springer Verlag (2006)
- [2] Eisenberg, Puschke, Singelstein: Überwachung mittels RFID-Technologie- Aspekte der Ausforschung und Kontrolle mit neuartigen Funk-Chips; ZRP 2005 Heft 1
- [3] Holznagel, Bonnekoh: Radio Frequency Identification - Innovation vs. Datenschutz? ; MMR 2006 Heft 1
- [4] Roßnagel: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung; MMR 2005 Heft 2
- [5] Tinnefeld: Vom archimedischen Punkt in einer Zivilgesellschaft; MMR 2004 Heft 12
- [6] Ari Juels, Ronald L Rivest, Michael Szydlo: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy (2003)
- [7] Simon L. Garfinkel, Ari Juels, Ravi Pappu: RFID Privacy: An Overview of Problems and Proposed Solutions (2005)
- [8] Roßnagel: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung MMR 2005 Heft 2

Literatur

- [9] Spiekermann, S.; Ziekow, H.: "RFID a Systematic Analysis of Privacy Threats & a 7-Point Plan to Adress Them" In: Journal of Information System Security, erscheint im Frühjahr 2006
- [10] Berthold, O.; Günther, O.; Spiekermann, S.:RFID-Technik: Verbraucherängste und Verbraucherschutz – eine Frage der Kontrolle
- [11] Juels, A.; Rivest, R.; Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy