



Vorlesung

Datenschutz und Privatheit in vernetzten Informationssystemen

Kapitel 6: Ubiquitous Computing
Teil 1: RFID

Erik Buchmann
buchmann@ipd.uka.de



Agenda für heute

[Einführung](#)

[RFID](#)

[Bedenken
bei RFID](#)

[Datenschutz-
ansätze](#)

[Abschluss](#)

- Einführung: Ubiquitous Computing
- Allgemeine Datenschutzprobleme in UbiComp-Szenarien
- RFID als wichtige aktuelle UbiComp-Technik
- Datenschutzprobleme in RFID-Szenarien
- Lösungsmöglichkeiten





Ursprünge des Ubiquitous Computing

[Einführung](#)

[RFID](#)

[Bedenken
bei RFID](#)

[Datenschutz-
ansätze](#)

[Abschluss](#)

- Marc Weiser, *The Computer for the 21st Century*, 1991
 - Zentrale Idee: Computer sollten nicht mehr die Aufmerksamkeit des Nutzers einfordern, sondern ihn selbständig und unmerklich im Alltag unterstützen
 - PC als Gegenstand der Aufmerksamkeit sollte verschwinden → Intelligente Alltagsgegenstände
- Ubicomp ist die 3. Welle der Computerisierung
 - 1. Mainframes
 - 2. PCs
 - 3. Ubicomp





Ubiquitous Computing

[Einführung](#)

[RFID](#)

[Bedenken
bei RFID](#)

[Datenschutz-
ansätze](#)

[Abschluss](#)

- Im wesentlichen ein Interaktionsmodell
 - Alltag durchdrungen von intelligenten Gegenständen
 - Gegenstände passen sich *Nutzer* und *Kontext* an
 - intelligente Dienste im Hintergrund
 - Minimum an expliziter Nutzerinteraktion
 - Dienste versuchen, Nutzerpräferenzen automatisch zu ermitteln und sinnvoll darauf zu reagieren





Abgrenzung zu verwandten Techniken

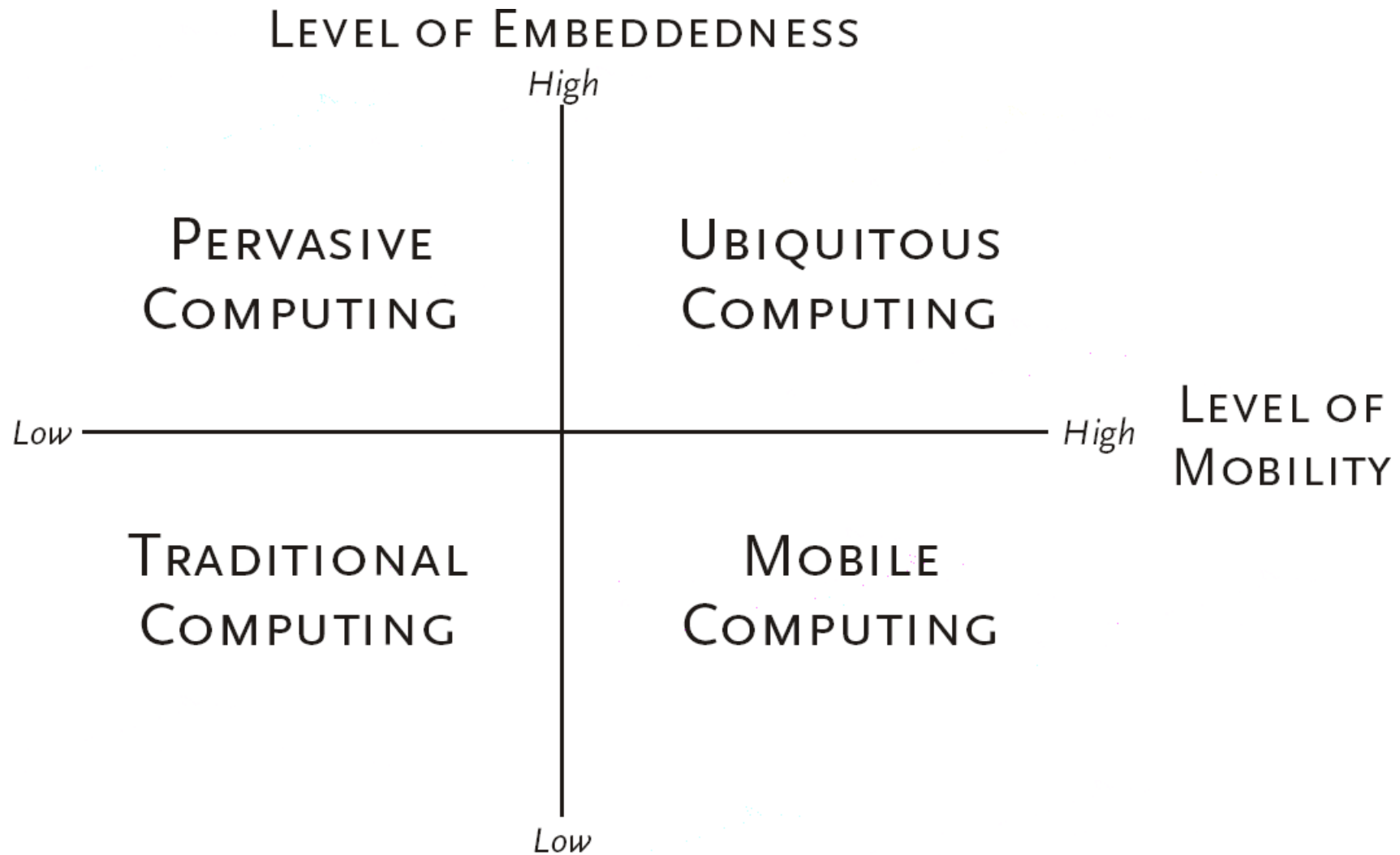
[Einführung](#)

[RFID](#)

[Bedenken bei RFID](#)

[Datenschutzansätze](#)

[Abschluss](#)



Quelle: Lyytinen, Yoo: Issues and Challenges in Ubicomp., CACM 2002





Eine typische Ubicomp-Anwendung

- Automatischer Visitenkartenaustausch bei Handschlag

Datenübertragung per Körperkontakt

Nächste News 

14:46 - 8. October 2002 von Stephan Lex  Empfehlen |  Drucken |  Kommentar |  Bookmark

Das japanische Unternehmen NTT DoCoMo hat ein Verfahren entwickelt, welches den Datenaustausch zwischen PDAs oder ähnlichem per Handschlag ermöglicht. Dabei wird die Leitfähigkeit der menschlichen Haut zur Übertragung schwacher elektrischer Signale genutzt. Nach Angaben von NTT DoCoMo erreicht man bisher eine Übertragungsrates von 10 MBit. Das Gerät wird über einen speziellen Sensor mit dem Träger verbunden und kann daher zum Datenaustausch in der Tasche bleiben, während beim Händeschütteln elektronische Visitenkarten getauscht werden. Das Verfahren könnte auch bei Personen- oder Ticketkontrollen genutzt werden.

Quelle: [Tom's Hardware](#)



Ubicomp-Techniken

[Einführung](#)

[RFID](#)

[Bedenken
bei RFID](#)

[Datenschutz-
ansätze](#)

[Abschluss](#)

- WLAN, Ad-Hoc Netze, Body Area Networks
- Mobiltelefone, XDAs, Wearables
- Embedded Systems, Intelligente Fahrzeuge
- Sensornetze, Mautbrücken
- Smart Homes, Smart Office
- GPS-Ortung, Lokationsbasierte Dienste
- RFID, Near Field Communication
 - *diese Vorlesung*





Eigenschaften von Ubicomp

[Einführung](#)

[RFID](#)

[Bedenken
bei RFID](#)

[Datenschutz-
ansätze](#)

[Abschluss](#)

- Stetige, überall verfügbare Computerunterstützung
 - Integration in den Alltag
- Stark vereinfachte Mensch-Maschine-Schnittstellen, die mit minimaler Nutzerinteraktion auskommen
 - “intelligente” Unterstützung im Hintergrund
- Automatische Steuerung; Anpassung an Nutzerpräferenzen und Kontext
- Automatische Ausführung von wiederkehrenden, standardisierten Abläufen ohne Nutzerinteraktion





Datenschutz und Ubiquitous Computing

[Einführung](#)

[RFID](#)

[Bedenken
bei RFID](#)

[Datenschutz-
ansätze](#)

[Abschluss](#)

- Ubicomp: KEINE ständige Kommunikation mit dem Benutzer
 - Anwendungen arbeiten im Hintergrund und “erraten” Nutzerwünsche
- Datenschutzrecht:
 - Zielt auf Nutzerinteraktion und -Beteiligung ab
 - Transparenz, Verbot mit Erlaubnisvorbehalt, Auskunftsansprüche

→ *Privacy Policies, Einverständniserklärungen stehen in fundamentalem Konflikt mit UbiComp!*



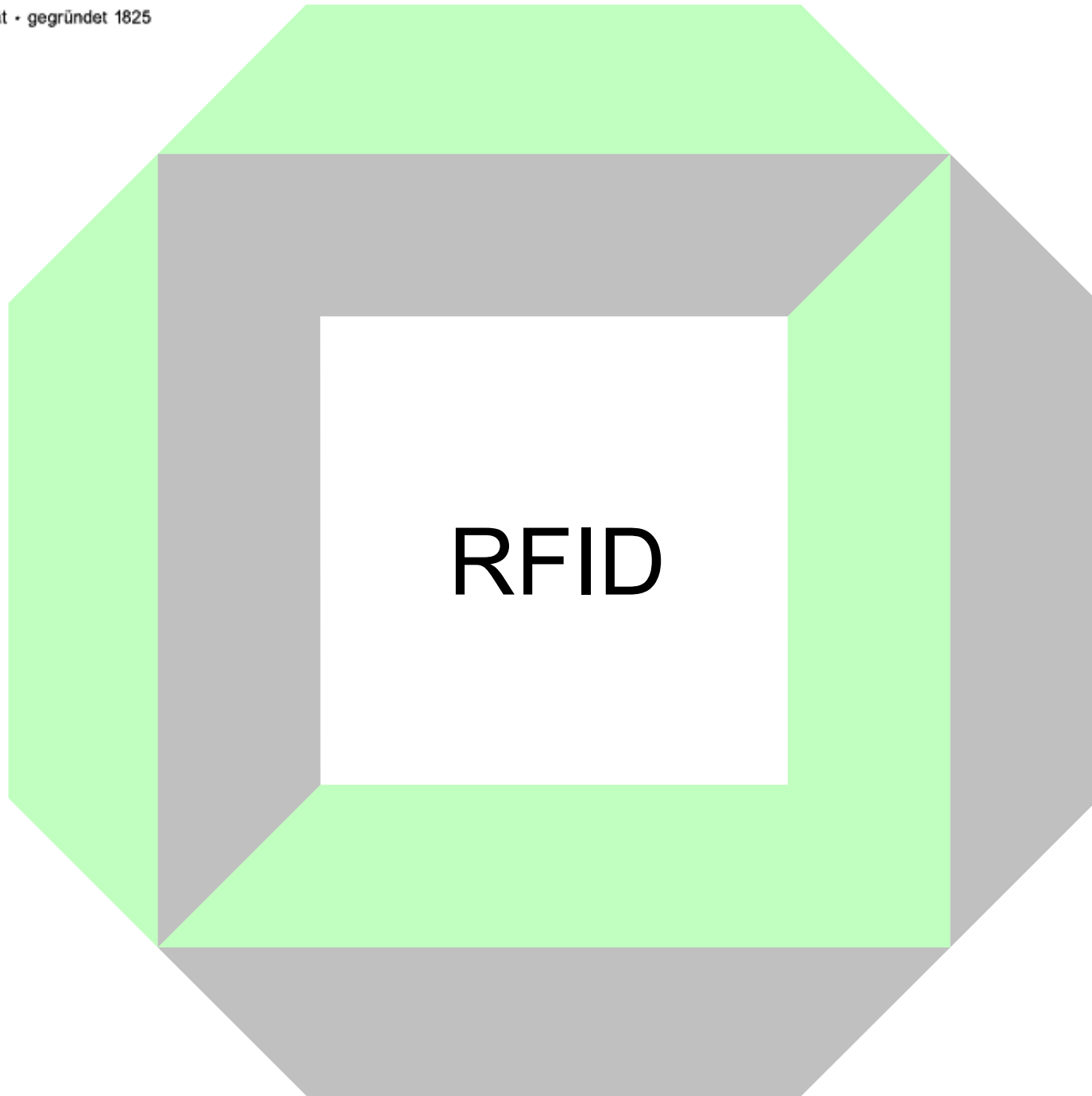


Aus einem Vortrag von Marc Langenheinrich

Approaches to Ubicomp Privacy

Disappearing Computer Troubadour Project (10/2002 - 05/2003)

- Promote Absence of Protection as **User Empowerment**
 - “It’s maybe about letting them find their own ways of cheating”
- Make it **Someone Else’s Problem**
 - “For [my colleague] it is more appropriate to think about [security and privacy] issues. It’s not really the case in my case”
- Insist that “**Good Security**” will Fix It
 - “All you need is really good firewalls”
- Conclude it is **Incompatible** with Ubiquitous Computing
 - “I think you can’t think of privacy... it’s impossible, because if I do it, I have troubles with finding [a] UbiComp future”





RFID

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Radio Frequency Identification
 - eine der heute weitverbreitetsten Ubicomp-Anwendungen
- Billige Funketiketten
 - global eindeutige ID
 - zum Teil wiederbeschreibbarer Speicher
 - zum Teil mit zusätzlichen Umweltsensoren
 - zum Teil mit Kryptografiefunktionen, Authentifizierung





RFID-Tags

Einführung

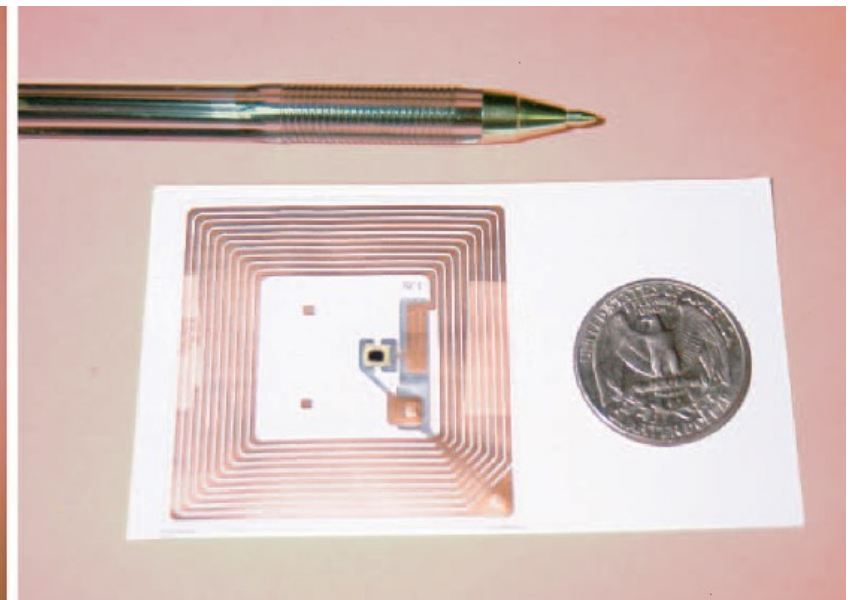
RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Eingeschmolzen in einen Glaskörper
 - robust, sogar in Lebewesen implantierbar
- Eingebettet in einen Aufkleber
 - Markierung von Paletten, Produkten etc.



Quelle: [2]





Passive und Aktive RFID Tags

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- **Passiv:**
 - geringe Reichweite
 - preiswerte Herstellung, klein
 - praktisch unbegrenzte Lebensdauer



- **Aktiv:**
 - hohe Reichweite
 - aufwändige Herstellung
 - benötigen Energiequelle,
z.B. Batterie oder Fahrzeug-Bordnetz





Anwendung: Tieridentifikation

Einführung

[RFID](#)

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss



Foto: Zoological Society of London



Anwendung: Reisepass (ePass)

- Biometrische Daten wie Passbild, Fingerabdruck elektronisch gespeichert
- Erweiterungen für Kryptografie und Authentifizierung



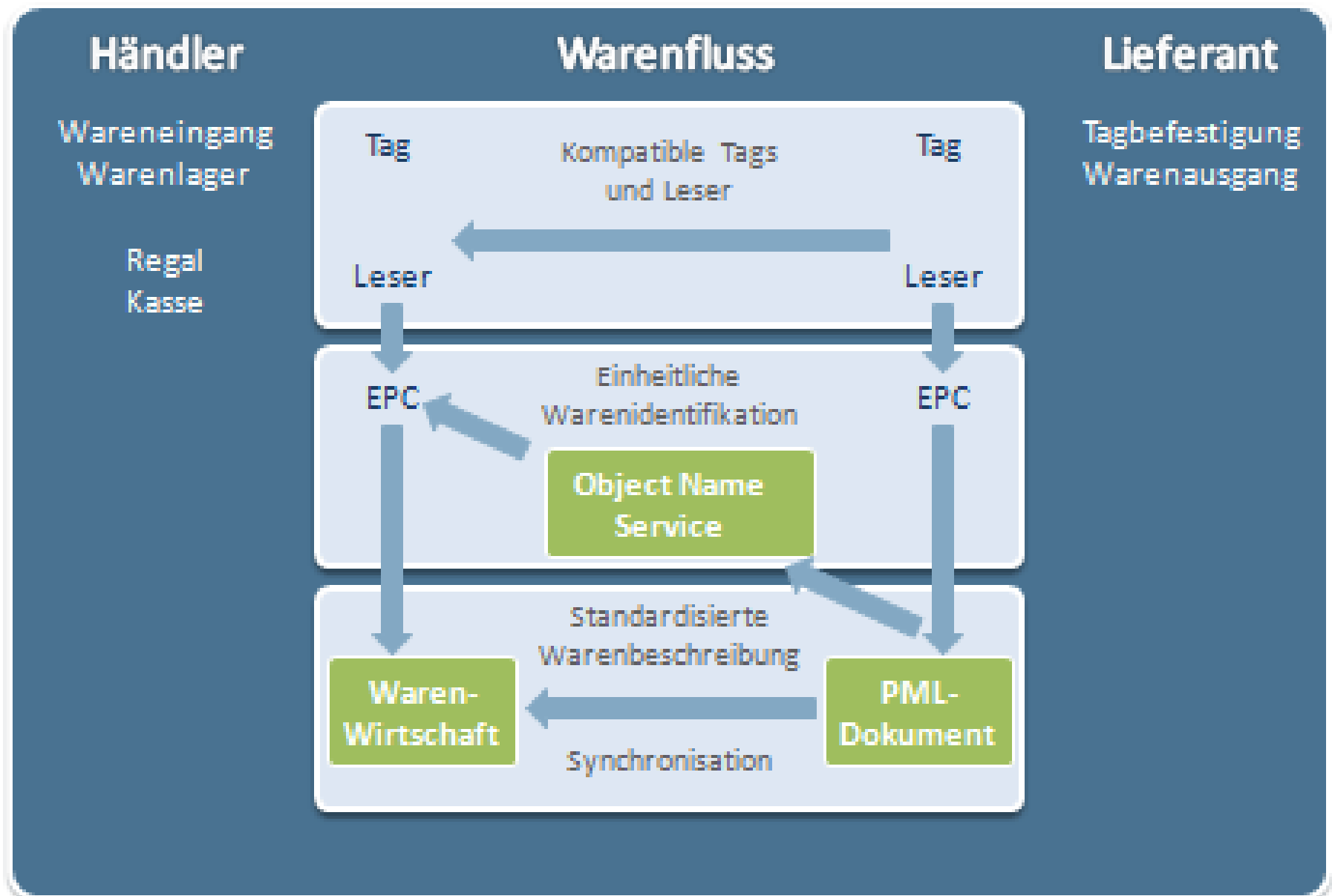
Anwendung: im Supermarkt

- jedes Produkt trägt einen eigenen RFID-Tag
- “Smart Shelf”
 - Regal mit RFID-Lesegeräten (unter den Regalböden)
- Anwendungen:
 - Planogramm Compliance
 - Inventur
 - vereinfachtes Kassieren

Bild: SAP Research, Karlsruhe



Anwendung: Supply Chain Management



Quelle: <http://www.rfid-basis.de>



Anwendung: Ablösung von Barcodes

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

Barcode

- Strichcode nach EAN-13: 12 Ziffern + 1 Prüfziffer
- speichert Produktgruppe
- auslesen erfordert direkte Sichtlinie
- muss sichtbar angebracht werden
- nicht beschreibbar
- müssen einzeln gelesen werden
- kosten praktisch nichts

RFID

- Smart Labels speichern aktuell 96kByte
- speichert eindeutige ID
- unbemerktes Auslesen aus Entfernung möglich
- Tags können sogar in die Haut implantiert werden
- wiederbeschreibbar
- mehrere Tags auf einmal lesbar
- ca. 30ct/Stück
(<http://www.rfid-basis.de>)

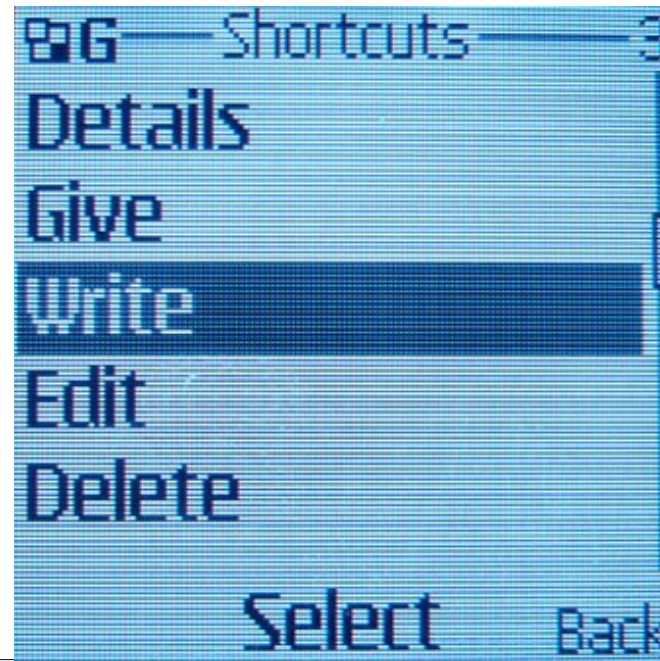
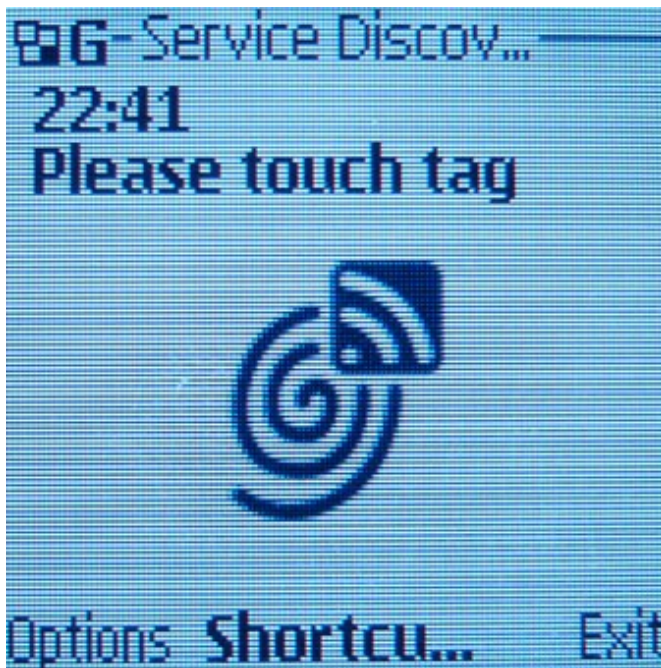


RFID-Leser: Nokia 3220 with NFC

- RFID als Träger von Texten, Telefonnummern, URLs



- Prototyp für ein Mobiltelefon
- mit Near Field Communication
- kann RFID lesen und schreiben



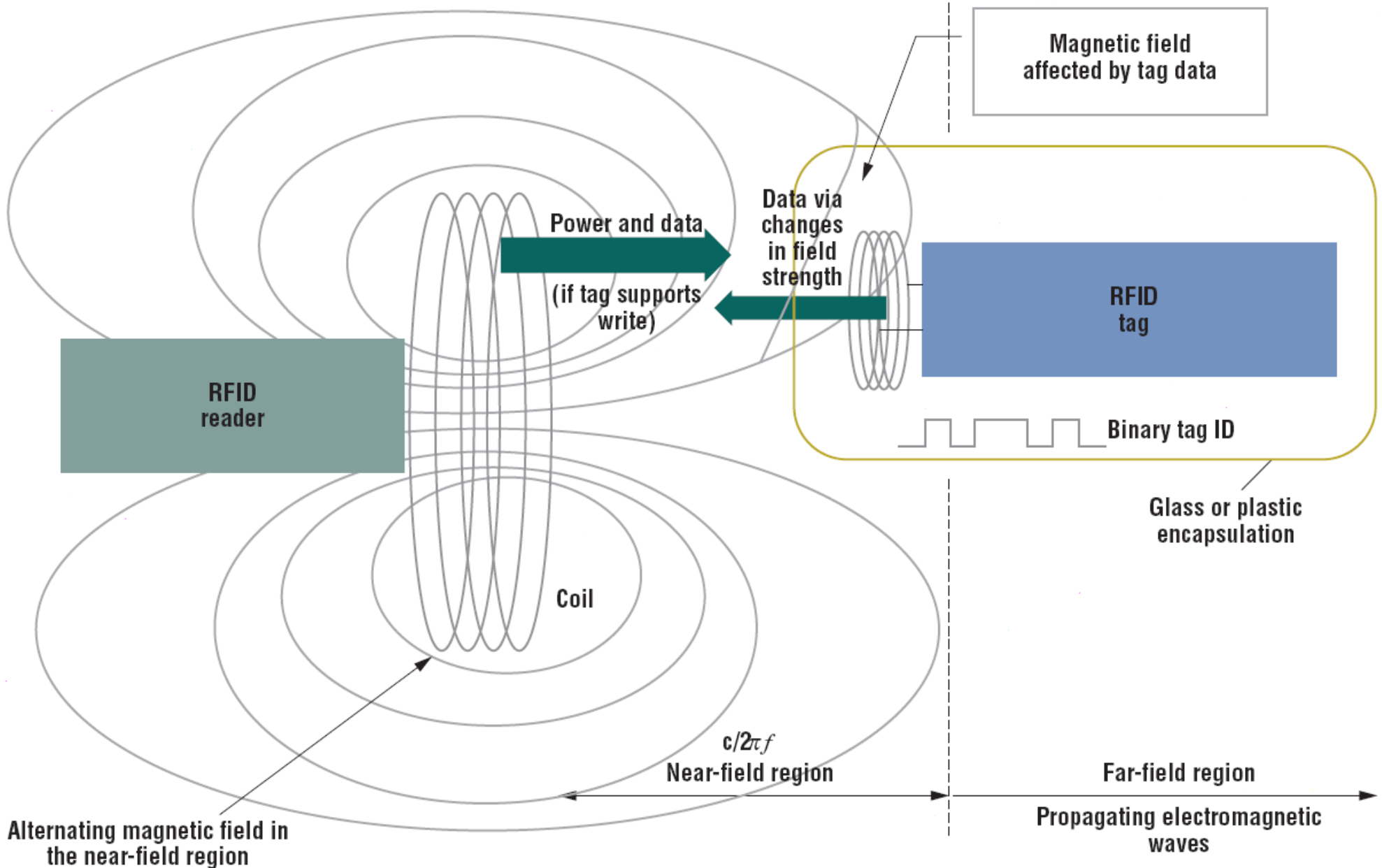


Funktionsweise von RFID



Funktionsweise passiver Tags

Using induction for power coupling from reader to tag and load modulation to transfer data from tag to reader





Typische Reichweiten

Einführung

[RFID](#)

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Close Coupling
 - Passive Tags, Reichweite 0-1cm, Transponder müssen in Lesegerät eingesteckt werden
 - Sicherheitskritische Anwendungen, z.B. FriCard
- Remote Coupling
 - Passive Tags, Reichweiten bis zu 1m
 - Einsatz z.B. im Supermarkt oder für Zutrittskontrolle
- Long Range
 - Reichweiten bis zu 10m
 - Aktive Tags, Energiequelle am Transponder nötig
 - Einsatz z.B. im Flottenmanagement





Die EPC-ID

Einführung

[RFID](#)

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- “Electronic Product Code”; Standardisierung der Daten im RFID-Tag
 - Interoperabilität zwischen Tags versch. Hersteller
- Für 96-Bit-Tags:

Header, techn. Angaben	Company Prefix	Item Reference	Serial Number
14 Bit, Länge, Typ, Struktur, Ver- sion, Genera- tion des EPC	20-40 Bit, Verweis auf Herausgeber der Tags	24-4 Bit, Produktkategorie	38 Bit, global eindeutige Produktnummer

- EPCglobal führt zentrale Datenbank mit Company-Prefixen und Produktkategorien
 - ONS: Object Naming Service, äquivalent zu DNS





Query Tree Protocol (1/3)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- *effiziente* Identifikation aller Tags in Reichweite des Lesegerätes
- EPCglobal generation-1 class-0 Tags
- Voraussetzungen:
 - jedes Tag hat eine global eindeutige ID
 - Lesegerät erkennt Kollisionen
 - mehrere Tags senden gleichzeitig





Query Tree Protocol (2/3)

Einführung

RFID

Bedenken
bei RFID

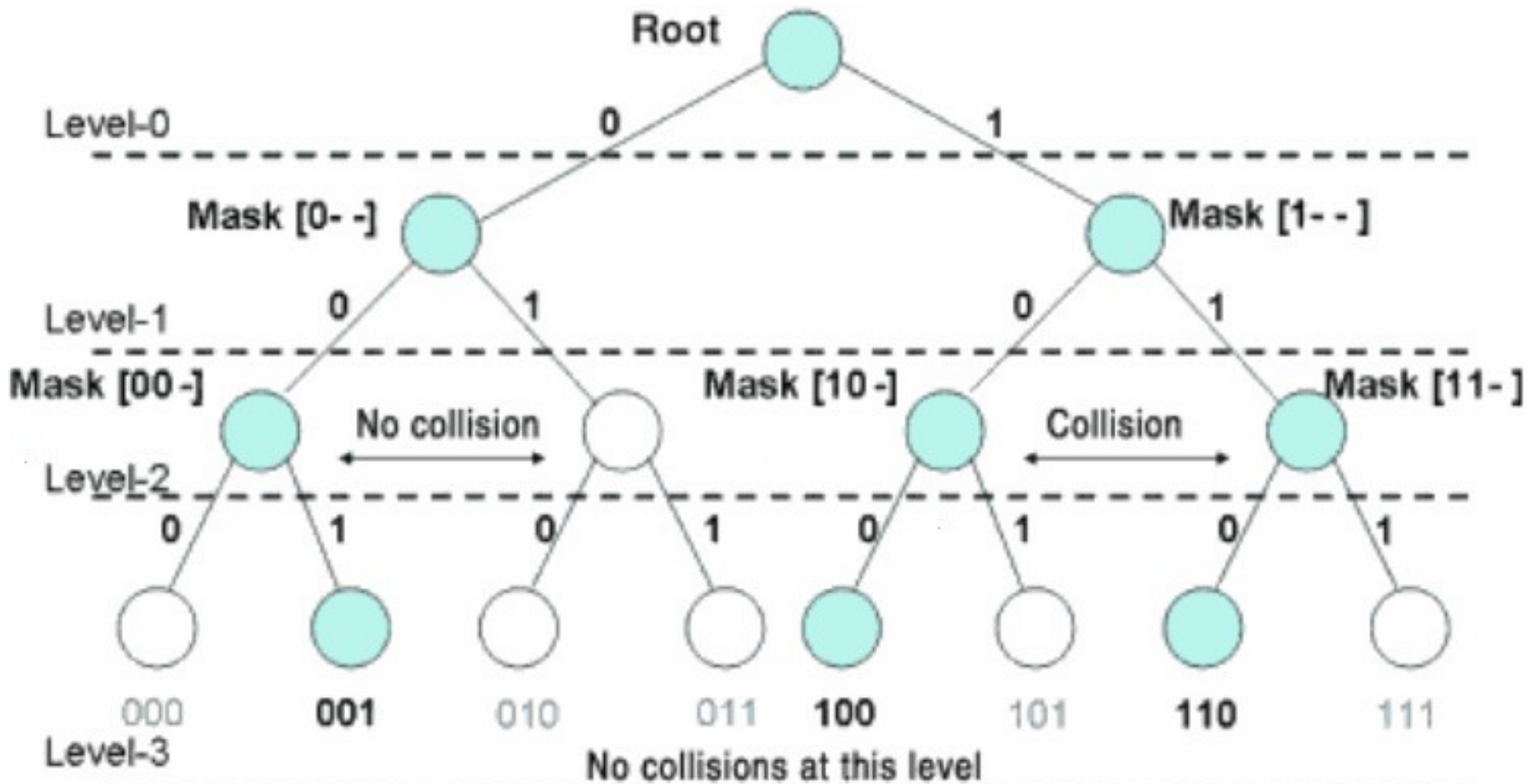
Datenschutz-
ansätze

Abschluss

- Leser sendet Bitmasken {0..., 1..., 00..., 01..., 10... etc.}
 - entspricht traversieren eines Baumes in Level-Order
- Jeder Tag, dessen ID-Prefix mit der Bitmaske übereinstimmt, antwortet
 - keine Antwort: Leser verfolgt diesen Zweig im Baum nicht weiter
 - genau eine Antwort: Tag sendet nächstes Bit seiner ID gleich mit
 - Leser fragt dann gezielt dieses Tag ab
 - Kollision (mehrere Antworten): Leser macht mit Level-Order Abfrage dieses Zweigs im Baum weiter



Query Tree Protocol (3/3)



Example using 3-bit tag IDs. Three tags 001, 100, and 110 are in bold
Note: At Level-3 all three tags can be successfully read using the masks [00-], [10-], [11-].

Quelle: RFID explained, Roy Want, 2006



Effizienz des Query Tree Protocols

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- es werden nur die Teile des ID-Raumes abgesucht, in denen Tags vorhanden sind
- Kostenabhängig von der Zahl der Kollisionen
 - Worst Case: viele Tags mit langem identischem Präfix in jeweils unterschiedlichen Zweigen des Baumes
- Erkennungsraten
 - bis zu 500 RFID-Tags pro Sekunde





Datenschutzbedenken beim Q.T.-Protokoll

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Lesegerät testet den gesamten Schlüsselraum, nicht nur die Tags, die beispielsweise im Laden verkauft werden
 - Ermittlung von allen Tags, die eine Person bei sich trägt
- Lesegerät sendet Tag-IDs mit voller Leistung
 - mit geeigneten Antennen über große Entfernungen (>50m) abhörbar





Query Slot Protocol (1/3)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- *effiziente* Identifikation aller Tags in Reichweite des Lesegerätes, *ohne* dass der Leser die Tag-ID mit voller Leistung senden muss
 - nur die Tags senden ihre ID, mit sehr viel geringerer Sendeleistung
- EPCglobal generation-2 Tags
- Voraussetzungen: jedes Tag besitzt
 - einen Zähler
 - ein Flag “Inventoried”
 - einen Zufallszahlengenerator





Query Slot Protocol (2/3)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Leser sendet einen QueryRequest mit Parameter Q
 - Alle Tags setzen Inventoried-Flag auf 0,
 - laden Counter mit Wert aus Zufallszahlengenerator Wertebereich $[0, 2^Q-1]$.
- Wenn ein Tag Counter = 0 hat
 - Tag generiert Zufallszahl, sendet sie an Leser
 - Wenn keine Kollision antwortet Leser mit der gleichen Zufallszahl
 - Tag antwortet mit seiner ID
 - Tag setzt Inventoried-Flag auf 1
 - Kollision: Tags suchen sich einen neuen Zufallslot
- Leser sendet QueryRep
 - Tags decrementieren Counter, Prozedur geht weiter



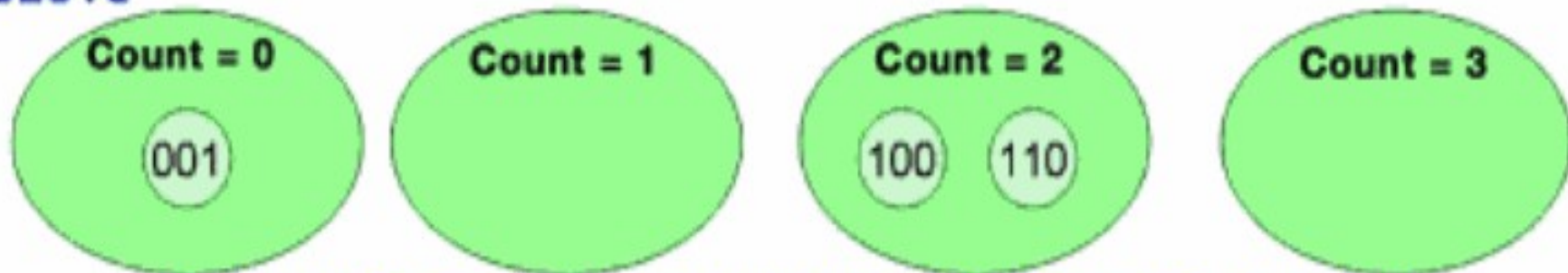
Query Slot Protocol (3/3)

Tags



1. Reader R: Sends query request with parameter: Q (Example $Q = 2$) and initiates an inventory round.
2. Tags $T()$: Load an internal slot counter with a random Q -bit number and clears inventoried flag.

SLOTS



Example $Q = 2$, resulting in four slots, RN16 is a 16-bit number

3. Tag with count=0 (e.g., 001) backscatters an RN16 random number.
4. Reader R: Acknowledges RN16 number.
5. Tag (e.g., 001) checks RN16 matches and backscatters EPC ID.
6. Reader R: Issues QueryRep command
Tag 001 set Inventoried Flag, and goes to sleep
Tags $T()$ remaining decrement slot count
Loop to 3 until $2^Q - 1$ QueryRep commands

Quelle: RFID explained, Roy Want, 2006



Effizienz des Query Slot Protocols

Einführung

[RFID](#)

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Hängt von der Anzahl der Tags und Parameter Q ab
 - Optimal: jedes Tag hat eigenen Slot, aber wenig unbesetzte Slots
 - In der Praxis: Leser testet mehrere Q, bis akzeptabler Kompromiss gefunden
- Erkennungsraten
 - bis zu 2000 Tags/Sekunde
(generation-2 Tags haben höhere Übertragungsgeschwindigkeit als generation-1)





Datenschutz und -sicherheit von RFID-Installationen



Was ist neu an RFID aus Datenschutzsicht?

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Auf den ersten Blick nicht viel
 - Bonuskarten an der Supermarktkasse erlauben vergleichbare Einblicke über das Kaufverhalten
- Aber:
 - Datenerfassung wird einfacher
 - nicht nur Erfassung an der Kasse, sondern unbemerkt an beliebiger Stelle
 - sehr feingranulare Daten
 - z.B. kann Smart Shelf registrieren, ob Produkt entfernt und zurückgelegt wird
 - elektronische Erfassung wird zum Standard und nicht zur Ausnahme
 - zahlreiche Sicherheitsbedenken (siehe Folgefolien)





Sicherheitsbedenken (1/2)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Passive RFID-Tags sind nach Kostengesichtspunkten entworfen → keine/kaum Sicherheitsfeatures
- **Sniffing**
 - Kommunikation zwischen Tag und Leser abhören
- **Spoofing und Replay-Attacken**
 - laufende Kommunikation manipulieren oder später wieder einspielen
- **Man-in-the-Middle-Attacken**
 - Angreifer schaltet sich in die Kommunikation ein
- **Cloning, Emulation**
 - fremden Transponder nachbauen bzw. emulieren





Sicherheitsbedenken (2/2)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- **Denial of Service**
 - RFID-Chip beschädigen, Lesefeld stören (jamming)
- **Tracking**
 - Bewegungsprofile durch Zuordnung der eindeutigen RFID-ID und Zeitpunkt der Lesung
- **Relay-Angriffe**
 - durch spezielle Antennen/elektronische Verstärkung Lesereichweite erhöhen, z.B. Anwesenheit einer Schlüsselkarte aus der Entfernung vortäuschen
- **RFID-Malware**
 - vgl. *Ist Ihre Katze mit einem Computervirus infiziert?*
Melanie R. Rieback, Bruno Crispo, A. Tanenbaum

- *Einzigster Schutz bisher: beschränkte Reichweite*





Datenschutzbedenken (1/2)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- **Action Threat** (Handlung)
 - durch Überwachung einer Gruppe von Tags kann auf die Absichten des Nutzers geschlossen werden
 - Beispiel: das gemeinsame Verschwinden von Tags auf teuren Produkten aus einem Smart Shelf könnte auf Ladendiebstahl hindeuten
- **Association Threat** (Zuordnung)
 - bei Kauf von RFID-markierten Gegenständen kann die Identität des Käufers mit der EPC-ID der Tags assoziiert werden
- **Location Threat** (Ort)
 - strategische Platzierung von RFID-Lesern
 - speichern von Ort, Zeit von vorbeikommenden Tags

Quelle: [3]





Datenschutzbedenken (2/2)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- **Preference Threat** (Vorlieben)
 - EPC-ID: Hersteller, Produkttyp und eindeutige ID
 - Vorlieben und ungef. Wert der Produkte auslesbar
- **Constellation Threat** (Zusammenstellung)
 - Wiedererkennen von Individuen durch charakteristische Zusammenstellung von mitgeführten RFID-Tags (in Kleidung, Schuhen, Geräten, etc.)
- **Transaction Threat** (Vorgang)
 - Übergang von Tags von einer Person zur nächsten erlaubt Rückschlüsse auf die Interaktion
- **Breadcrumb Threat** (Spuren)
 - Falsche Spuren durch entwenden oder clonen von Tags, die anderen Personen zugeordnet sind

Quelle: [3]





Datenschutz-Ansätze für RFID

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- auf der gesellschaftlichen Ebene
 - Regeln zum “fairen” Umgang mit RFID
- auf der Hardware-Ebene
 - Metallgehäuse, Abbrechantennen, etc.
- auf der Software-Ebene
 - Kill-Befehl, Tag-Pseudonyms etc.
- *Achtung, untersch. Anforderungen je nach Anwendung!*
 - soll das Tag unbeschädigt (Reisepass) bleiben?
 - soll das Tag auslesbar (Reklamation) bleiben?





RFID Bill of Rights

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- S. Garfinkel, 2002, in Anlehnung an die OECD-Empfehlungen:
 - das Recht zu wissen, ob Produkte RFID-Tags enthalten
 - das Recht, RFID-Tags beim Einkauf entfernen oder deaktivieren zu lassen
 - das Recht, RFID-unterstützte Dienste auch ohne RFID zu nutzen
 - das Recht, auf die Daten im RFID-Tag zuzugreifen
 - das Recht zu wissen, wann, wo und warum Tags gelesen werden





Metallhülle

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Metallhülle schirmt die Antenne der Tags ab
 - Störung der Energieversorgung und Kommunikation der Tags
 - z.B. kommerziell verfügbar für aktuelle Reisepässe
- Vorteile
 - einfache Kontrolle (Tag in Hülle oder nicht)
 - nach belieben aktivierbar/deaktivierbar
- Nachteile
 - nur für wenige Anwendungen geeignet, z.B. nicht für Tags, die in Kleidung eingewebt sind





PCB: Physically Changeable Bit

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Cliff C. Zou, *PCB: Physically Changeable Bit for Preserving Privacy in Low-End RFID Tags*, University of Central Florida, 2006
- Grundprinzip: ein einfacher Schalter
 - z.B. zwischen Antenne und RFID-Tag
 - auch mehrere Schalter möglich, um Ausleserechte detaillierter festzulegen
- Vorteile
 - reversibel
 - vergleichsweise leicht zu kontrollieren, kommt auf die Realisierung des Schalters an
- Nachteile
 - macht das Tag teuer





Clipped Tags

Einführung

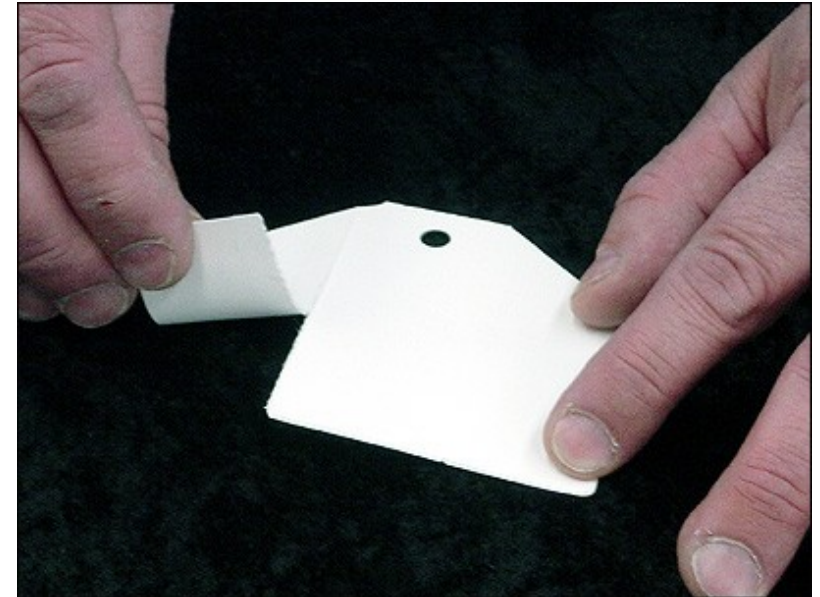
RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Patent von IBM
- mechanische Beschädigung des Tags
 - z.B. realisiert als Antenne zum Abreißen
- Vorteile
 - leicht kontrollierbar
 - Chip und Daten selbst bleiben unbeschädigt, Auslesen aus wenigen Millimetern noch möglich
- Nachteile
 - permanent
 - unbemerktes Auslesen möglich, nur Hürde ist höher





Kill-Befehl

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Standardisiert in EPCglobal generation-2 Tags
 - jedes Tag enthält ein 32-Bit-Passwort
 - Leser kann nach Passwortauthentifizierung den Chip permanent deaktivieren
- Vorteile
 - keine Nutzerinteraktion erforderlich
 - mehrere Tags gleichzeitig deaktivieren
- Nachteile
 - permanent
 - schwer zu kontrollieren





RFID-Zapper

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- 2006 auf dem 22. Chaos Communication Congress vorgestellt
- sendet einen starken elektromagnetischen Puls aus, der RFID-Chips auf kurze Entfernung zerstört
- Vorteile
 - nicht Hersteller /Distributor abhängig
- Nachteile
 - Erfolg nicht kontrollierbar
 - permanent



Bild: <http://www.extremflug.de>





Tag Pseudonyms

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Ziel: verhindern einer Zuordnung von Tags zu Personen durch Unberechtigte
- Idee: jedes Tag verfügt über zahlreiche verschiedene IDs, die zufällig benutzt werden
 - bei jedem Lesevorgang scheint sich ein anderes Tag zu melden
 - nur der Herausgeber der Tags hat alle Pseudonyme in seiner Datenbank und kann sie eindeutig zuordnen
- Vorteile
 - leicht implementierbar
- Nachteile
 - langes mithören → alle Pseudonyme erkennbar
 - hilft nur gegen unberechtigtes Abhören, nicht gegen Datensammlungen vom Tag-Herausgeber





Blocker Tags

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- modifiziertes RFID-Tag
 - hält Funkstille bei autorisierten RFID-Lesern
 - blockiert unautorisierte RFID-Leser
 - meldet sich für jeden beliebigen Präfix
 - blockiert Identifikation, weil der Leser nun sämtliche theoretisch möglichen Adressen durchprobieren muss
→ 2^{96} für class-1 tags, vgl. Query Tree Protocol
- Varianten neben dem vollständigen Blocken:
 - Privacy-Zonen
 - Polite Blocking
 - Soft Blocking

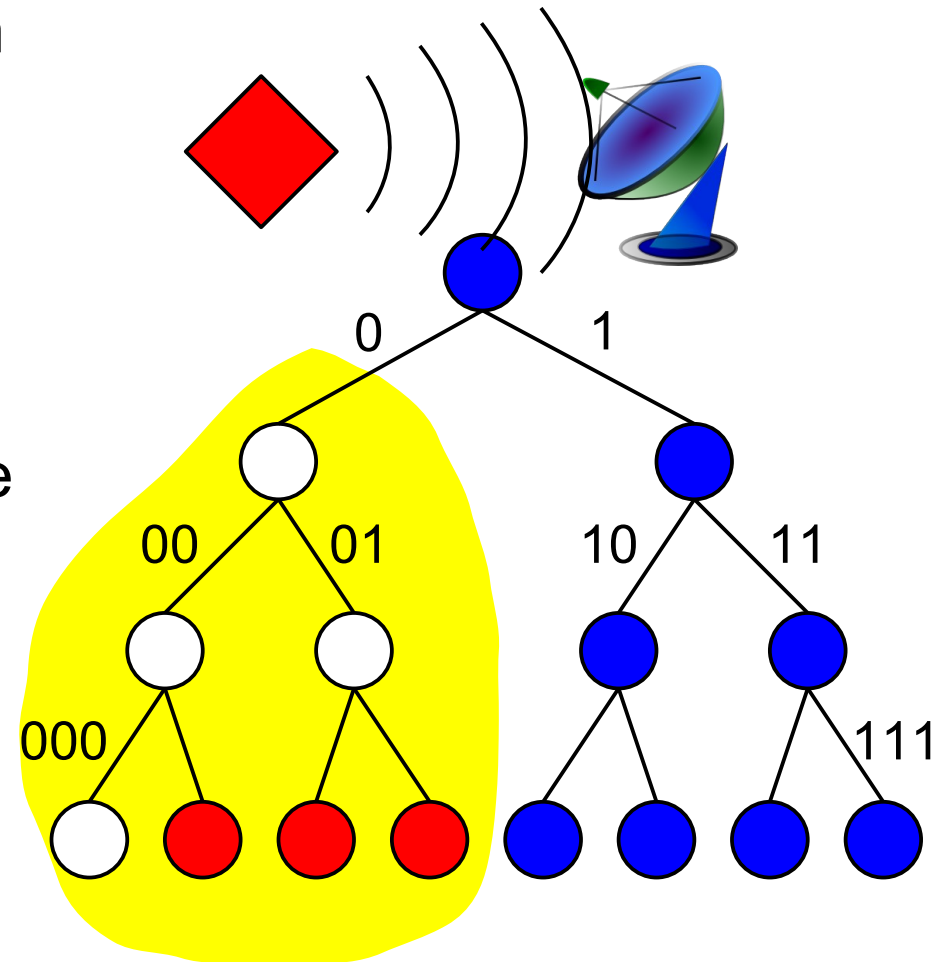




Privacy-Zonen

Einführung
RFID
Bedenken
bei RFID
[Datenschutz-
ansätze](#)
Abschluss

- nur bestimmte Teilbäume werden geblockt
 - Blocker-Tag sendet nur bei vorher ausgewählten Präfixen
- Vorteile
 - keine vollständige Blockade
- Nachteile
 - wenn große Teilbäume geblockt werden, dauert Identifikation der erlaubten Tags extrem lange
 - erlaubte Tags werden ggf. mit blockiert

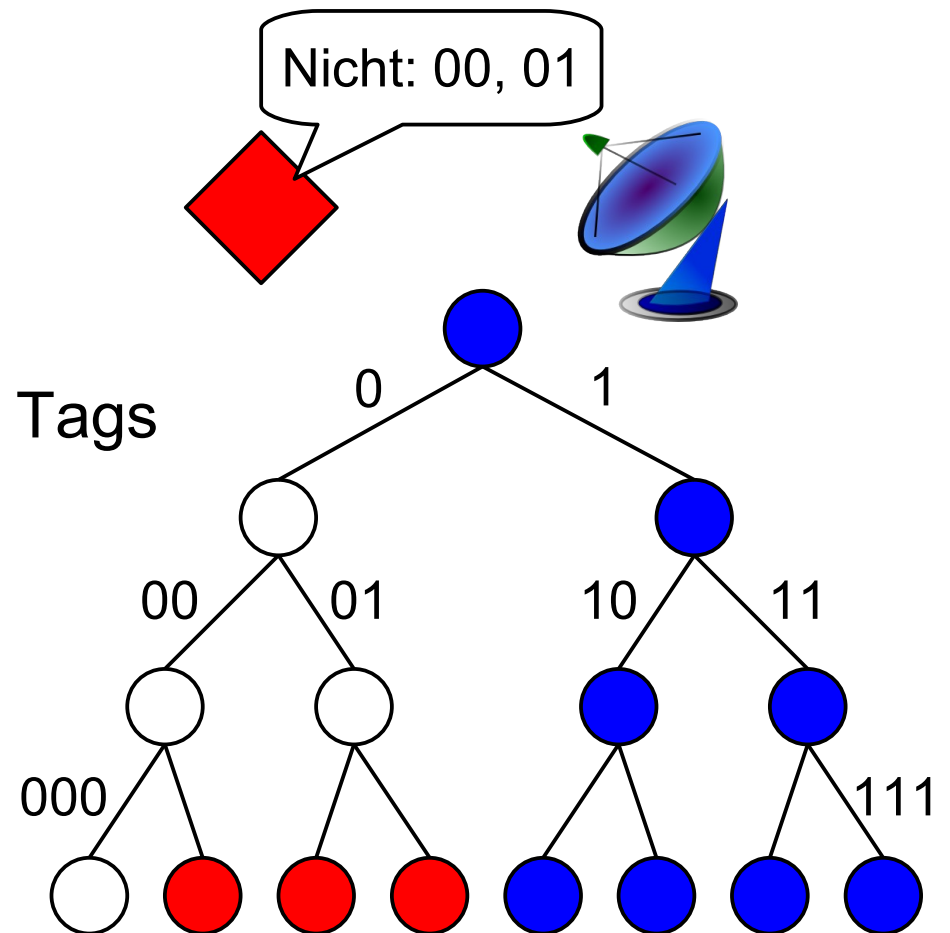




Polite Blocking

Einführung
RFID
Bedenken
bei RFID
[Datenschutz-
ansätze](#)
Abschluss

- Blockertag teilt Leser mit, welche Präfixe nicht abgesucht werden sollen
- Vorteile
 - keine vollständige Blockade
 - behindert nicht den Lesevorgang erlaubter Tags
- Nachteile
 - Implementierungsaufwand beim Leser

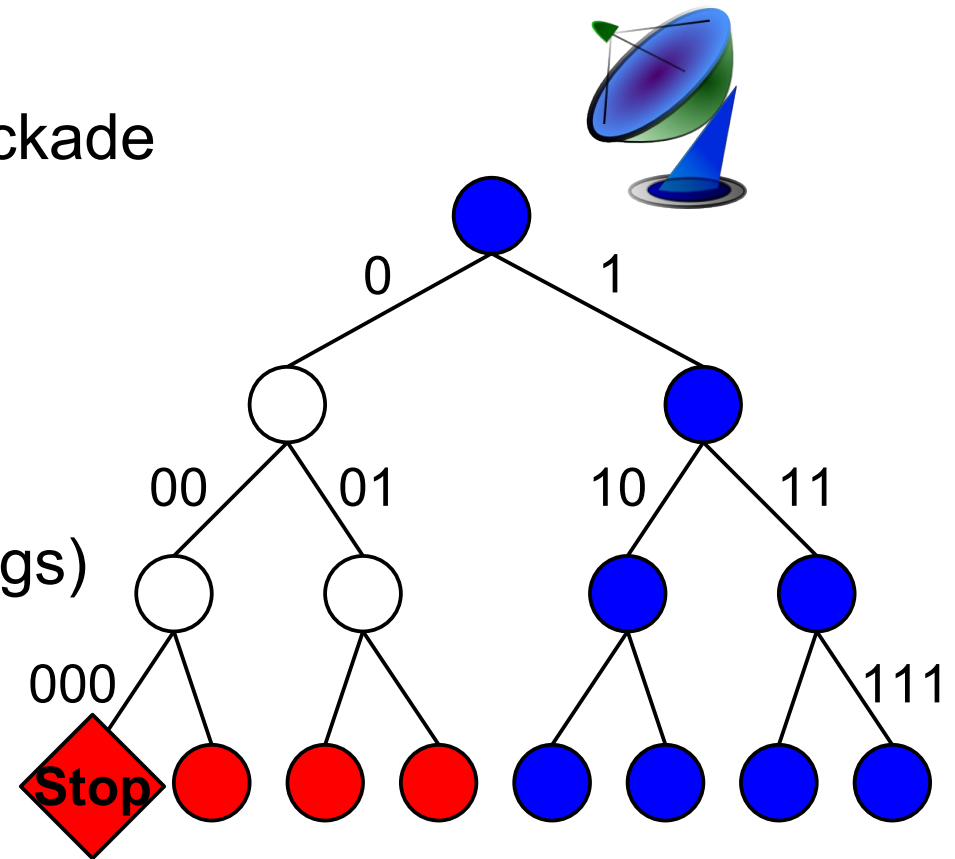




Soft Blocking

- Einführung
- RFID
- Bedenken bei RFID
- [Datenschutzansätze](#)
- Abschluss

- Spezielle Tags mit Adressbereichen, die vor den privaten Tags kommen, teilen dem Leser mit, dass er nicht weiter scannen darf
- Vorteile
 - keine vollständige Blockade
 - leicht implementierbar
 - behindert nicht den Lesevorgang
 - billige Blocker Tags (markierte normale Tags)
- Nachteile
 - Einhaltung unkontrollierbar





Umsetzung von P3P auf RFID (1/2)

Einführung

RFID

Bedenken bei RFID

Datenschutzansätze

Abschluss

- Erweiterung des Inventory-Kommandos
 - Leser sendet Informationen zu Datensammler, eine Policy-ID, eine binär kodierte kompakte Policy und eine ID des Lesegeräts
- Watchdog-Tag
 - lädt die Policy anhand der ID übers Internet
 - vergleicht Nutzerpräferenzen mit Policy, blockiert ggf. Identifikationsvorgang

Protocol extension	Init round all	SUID flag	Round size	CRC-5	RPID	Purpose	Collection type	CRC-16
1 bit	6 bits	1 bit	3 bits	5 bits	96 bits	16 bits	2 bits	16 bits

Header	Data Collector	Policy	Reader
8 bits	28 bit	24 bits	36 bits

The modified inventory command, Init_round_all

C. Floerkemeier et al.,
Scanning with a Purpose, UCS'2004





Umsetzung von P3P auf RFID (2/2)

Einführung

RFID

Bedenken
bei RFID

Datenschutz-
ansätze

Abschluss

- Vorteile
 - ausgefeilte Policy-Spezifikationen möglich
- Nachteile
 - wie P3P, also keine Mechanismen zur Durchsetzung, schwierige Bedienung, erfordert Expertenwissen beim Nutzer
 - komplizierte Realisierung
 - teure Infrastruktur aus Watchdogs, Policy-Servern und mobiler Internet-Anbindung
 - große Erweiterungen an Lesegeräten, Tags und Protokollen erforderlich





Abschluss Ubicomp. Teil 1



Zusammenfassung

[Einführung](#)

[RFID](#)

[Bedenken
bei RFID](#)

[Datenschutz-
ansätze](#)

[Abschluss](#)

- RFID ist eine der derzeit populärsten Ubicomp-Techniken
- Funktionsweise von RFID
- Zahlreiche Datenschutz- und Sicherheitsbedenken
 - resultierend aus den technischen Fähigkeiten und der Forderung nach billigen Tags
- Weites Spektrum an Lösungsmöglichkeiten





Literatur

- [1] *TAUCIS: Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung*, Studie für das BMBF
https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf
- [2] Roy Wart, *An Introduction to RFID Technology*,
IEEE Pervasive Computing 2006
- [3] Simson Garfinkel et al., *RFID Privacy: An Overview of Problems and Proposed Solutions*,
IEEE Security and Privacy 2005

