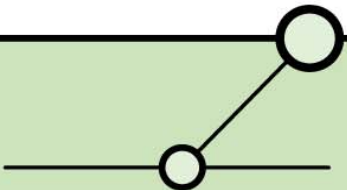
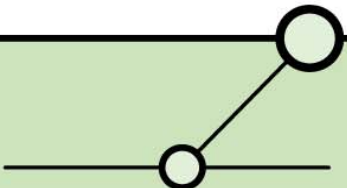


# RFID Security

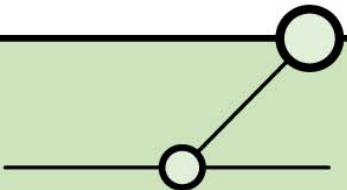
Enno Rey, [erey@ernw.de](mailto:erey@ernw.de)  
CISSP, CISA



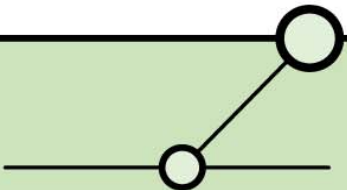
- Gegründet Sommer 2001 durch Enno Rey
- Netzwerk-Dienstleister mit Sicherheits-Fokus
- Aktuell neun Mitarbeiter
- Schwerpunkte: Security Management, Audit/Revision, Penetrations-Tests, Risiko-Bewertung & -Management, Security Research
- Kunden: Industrie, Banken, Behörden, Provider
- [www.ernw.de](http://www.ernw.de)



- Einführung RFID
- Strukturelle Sicherheitsaspekte
- Angriffe & mögliche Sicherheitsprobleme

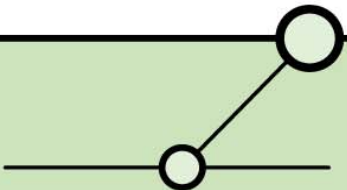


- RFID: *Radio Frequency Identification*
- Technologie zur Identifikation von Objekten durch Radiowellen.
- Kleine Geräte (*Tags, Transponder*), die über Funk eine Kennung senden, wenn sie (von einem *Reader*) *angesprochen* werden.
- Diese Geräte verfügen inzwischen über Speicher (unterschiedlicher Grösse), der beschrieben und ausgelesen werden kann.
- => kontaktlose Technologie zum Datenaustausch zwischen Datenträger und Lesegerät.

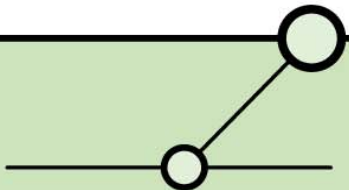
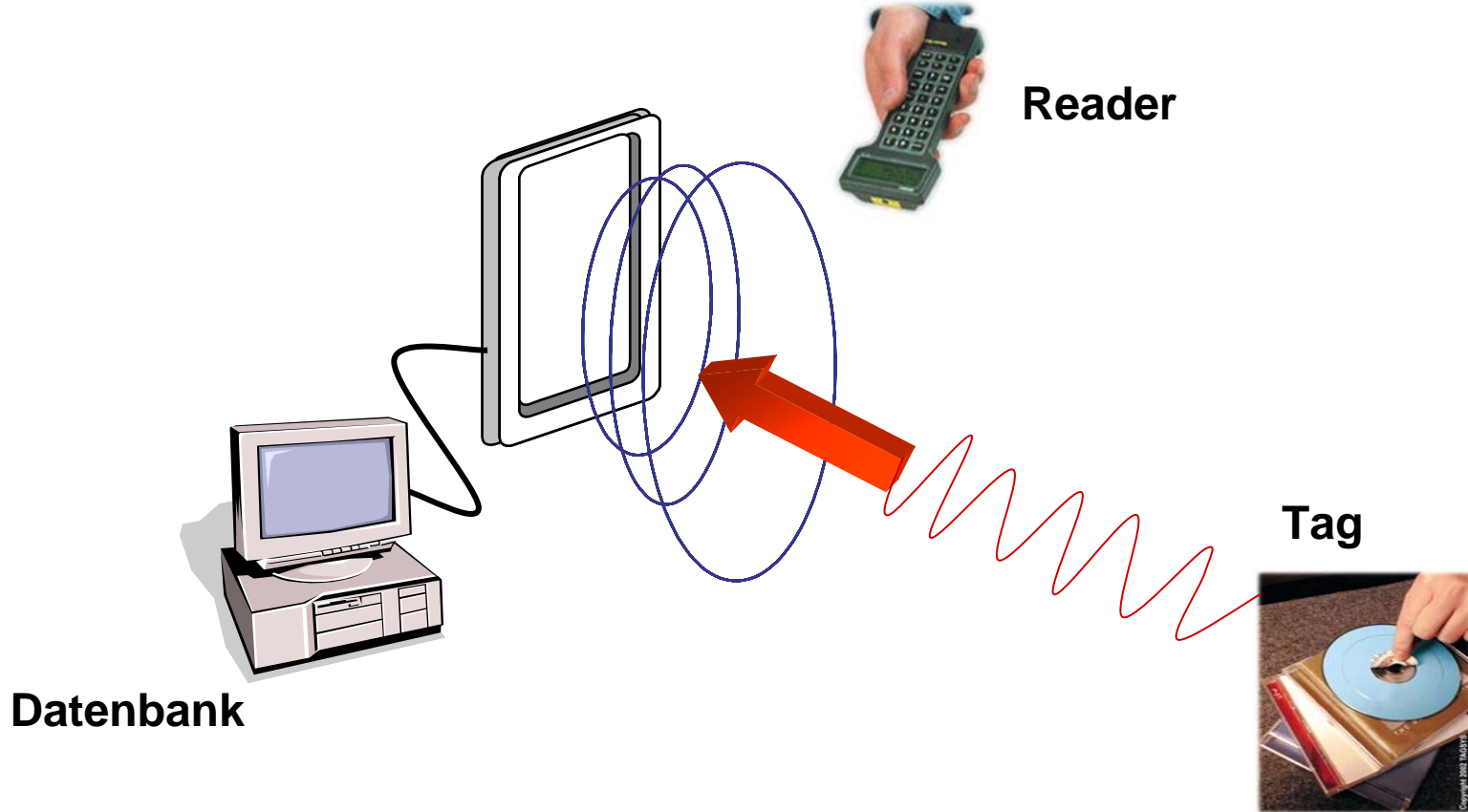


Drei Komponenten sind beteiligt:

- Ein *Tag* mit Chip & Antenne.
- Ein *Reader* (der üblicherweise auch schreiben kann) mit Antenne, Prozessor und Schnittstelle zum...
- *Informationsverarbeitendem System*, etwa einer Datenbank-Applikation.

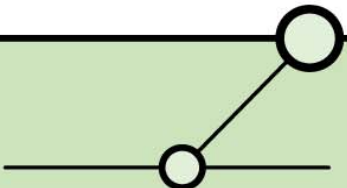


# Einführung RFID



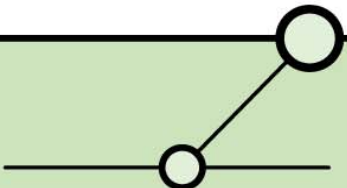
Tags können u.a. unterschieden werden nach:

- Stromversorgung: *aktiv* (Batterie) vs. *passiv* (induktive Kopplung)
  - Art (Read-Only, WORM, RW) & Größe des Speichers (1 Bit – 64 KBit)
  - Verwendetem Frequenzbereich & Reichweite
  - Methode der Datenübertragung
- 
- Besondere Aufmerksamkeit geniessen aktuell passive Tags, die mit der Frequenz 13,56 MHz arbeiten (oft *Smart Labels* genannt).
  - => sie bilden auch den Fokus dieses Vortrags.



*„The nice thing about standards is that there are so many to choose from. And if you really don't like all the standards you just have to wait another year until the one arises you are looking for.“ (A. Tanenbaum)*

- Zu RFID existiert eine Unmenge verschiedener Standards von verschiedensten Organisationen (ISO, IEC, ANSI etc.).
- Die hier wichtigsten sind:
  - ISO 14443 *Proximity Cards*
  - ISO 15693 *Vicinity Cards*
  - ISO 15962 *RFID for item management -- Data protocol*
  - ISO 18000-3 *RFID for item management -- Air interface comm. at 13,56 MHz*



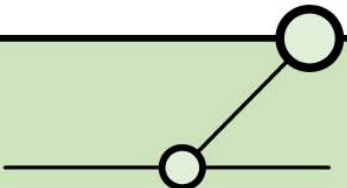
## Speicheraufbau eines ISO-15693-Tags

Address	Page							
	01	02	03	04	05	06	07	
0x00	Serial (UID)			MFR		0xE0		Administrativer Block
0x00								User-Block
0x01								
0x02								User-Data
...								...
0x7F								User-Data

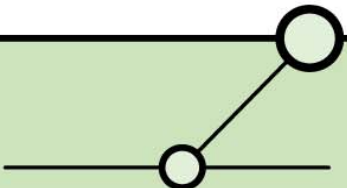
MFR – Hersteller ID

entnommen aus [1]

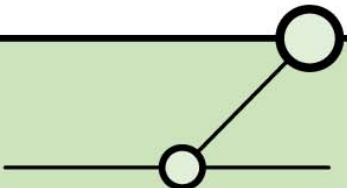
- ISO 18000-3 spezifiziert grundsätzlich (u.a.) *Read & Write*-Kommandos.
- Darüber hinaus können Speicherbereiche mit Schreibschutz (*lock*) versehen werden.
- Dieser Schreibschutz ist irreversibel, bei *Mode 2* Tags ist der Lock-Vorgang jedoch mit einem 48Bit-Kennwort geschützt.
- Nur *unlocked* Bereiche können (z.B. mit *rfdump*) überschrieben werden.
- Allerdings wird der Schreibschutz-Mechanismus aktuell kaum eingesetzt.
  
- Die *EPC*-Spezifikation (s.u.) sieht auch ein (Passwort-geschütztes) *Kill*-Kommando vor, mit dem Tags komplett deaktiviert werden (etwa zum Schutz der *Privacy*).
- Dieses *Kill* steht aber vielen sinnvollen Nutzungsmöglichkeiten im Weg...  
=> grossflächige Umsetzung diskussionswürdig & fraglich.



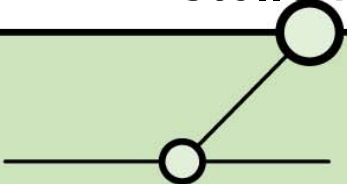
- Im Rahmen der *Supply Chain* (etwa für Waren-Paletten)
- Ersatz von Barcodes durch Tags + *Electronic Product Code* (EPC)
- In Bibliotheken
- Inventory
- Identifizierung von Besuchern/Gästen
- Abrechnung von Leistungen (Freizeitparks)
- Bei der Gepäckabfertigung an Flughäfen
- Animal Tagging
- usw. usw.



- Wir diskutieren hier nicht, ob eine Technologie ‚gut‘ oder ‚schlecht‘ ist.
- Unter Security-Gesichtspunkten ist nur relevant:  
Welche (neuen) Risiken ergeben sich?  
Wie sind diese zu bewerten?  
Ist der Einsatz der Technologie also gemäss den Sicherheitsanforderungen der Organisation angemessen?



- RFID Tags sind Träger von Informationen. Und damit von *Unternehmenswerten*.  
Typische Kriterien bei der Risiko-Analyse von Informationen sind etwa:
    - Kosten für die Produktion der Information.
    - Wert der Information für den Geschäftszweck.
    - Beeinträchtigung des Geschäftszwecks, falls die Information nicht verfügbar wäre.
    - !! Vorteil, den ein Mitbewerber erzielen könnte, falls er die Information nutzen, verändern oder zerstören könnte?
    - !! Kosten für die Organisation, falls die Information veröffentlicht, geändert, zerstört würde.
    - Verlust von Kundenvertrauen, falls die Information nicht sicher gespeichert oder verarbeitet würde.
- => stellen Sie sich diese Fragen!

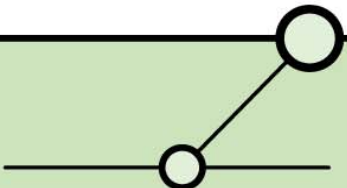


Im Grunde ergeben sich für die auf Tags gespeicherten Daten die üblichen Sicherheitsziele:

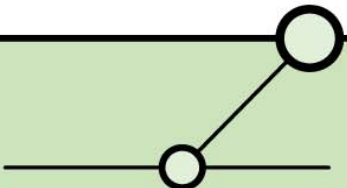
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität (etwa zum Schutz vor Produktfälschungen)

... aber mit ...

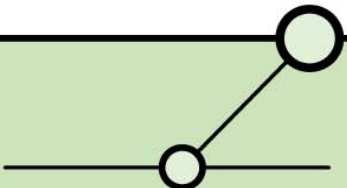
- schlechten Rahmenbedingungen
- ggf. neuen Angriffsmethoden



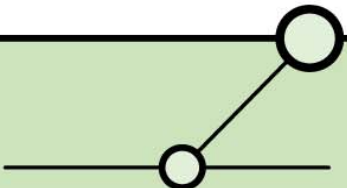
- Passive Tags haben nur Strom, solange sie im Radius des Lesers sind
  - => wenig Zeit für Berechnungen (Krypto)
  - => weniger Schutzmechanismen möglich
- Sie haben nur wenige (500-5000) *Gates* => kaum kryptographische Funktionalität
- Kaum physische Sicherheit (im Ggs. etwa zu Smart Cards)
- Wg. des avisierten Massen-Einsatzes ist ein harter Preiskampf zu erwarten
  - => Sicherheit bleibt auf der Strecke



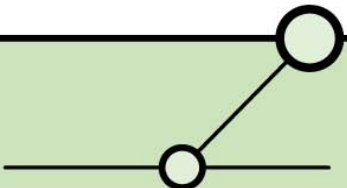
- Mitlesen des (Funk-) Verkehrs zwischen Tag und Reader
- Unautorisiertes Lesen oder Ändern von Daten
- Neue *Side Channel* Attacken (gegen höherwertige RFID-Implementierungen).



- Prinzipiell handelt es sich um typisches Sniffing einer Funk-Strecke.
- Jedoch Asymmetrie hinsichtlich Entfernung zwischen *Forward Channel* (Reader -> Tag) und *Backward Channel* (Tag -> Reader).
- Gilt zumindest für *Smart Labels* aufgrund der geringen Entfernung aktuell als wenig gefährlich.
- Aber: Entfernung hängt von Power und Antenne ab  
=> beides kann Angreifer potentiell steuern (siehe WLANs).

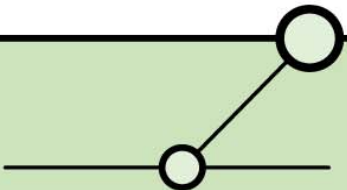


- Mit einem geeigneten Reader kann ein Angreifer üblicherweise Tags auslesen (Ausnahme: höherwertige Tags mit Krypto-Funktionen [z.B. Zugangskontrolle]).
- Ermöglicht wird dies durch fehlende Zugriffskontroll-Mechanismen.
- Oft ist (aufgrund des vernachlässigten Schreibschutzes) auch ein Beschreiben von Tags möglich (etwa mit *rfdump*).
- Mögliche Angriffsszenarien:
  - Informationsermittlung im Rahmen der *Supply Chain*
  - Inventory... durch Mitbewerber
  - Manipulation von Preisen oder Umdeklarierung von Waren
  - Umleiten/Entfernen von Gepäckstücken
  - Produktfälschung mit geclonten Tags
  - etc.

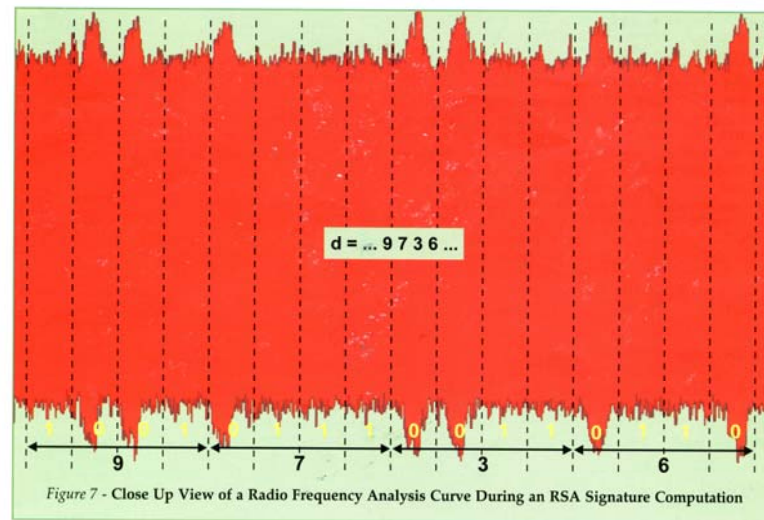
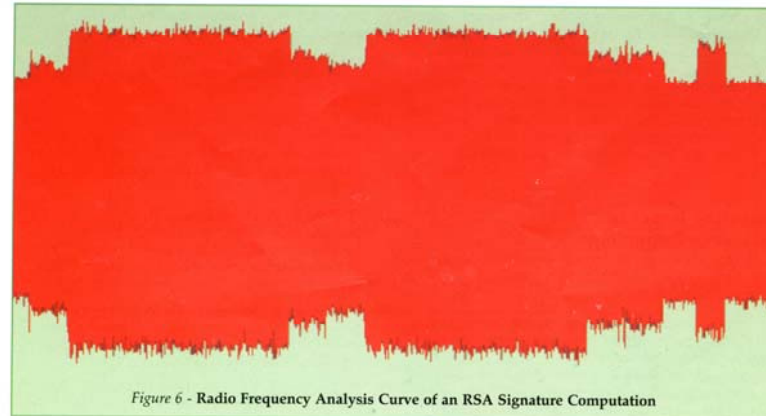


# Neue *Side Channel* Attacken

- Neue Technologien ermöglichen potentiell neue Angriffstypen.
- Gegen RFID/kontaktlose Technologien z.B. neue *Side Channel* Attacken.
- Siehe etwa Forschungsergebnisse von Helena Handschuh/Gemplus [2].

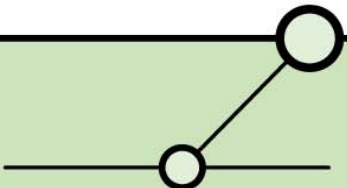


# Radio Frequency Analysis

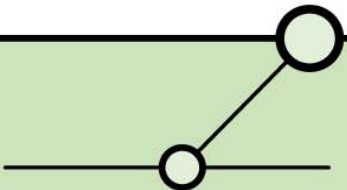


entnommen aus [2]

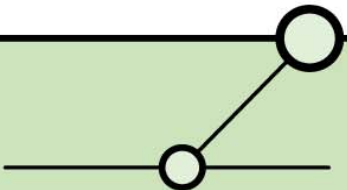
- Viele der hier genannten Probleme entstehen durch den Einsatz unauthorisierter Reader  
=> ggf. sollten sich Reader authentifizieren (als datenverarbeitende Devices übrigens auch *im* Netz...)  
=> Mechanismen zur Entdeckung von *rogue readers* sollten je nach Einsatz implementiert werden. Hier gibt es verschiedene Ansätze (etwa [3]).
- Die technischen Limitierungen von *Smart Labels* und die sich daraus ergebenden Angriffsszenarien sowie neue Angriffsmethoden gegen kontaktlose Technologien sollten bedacht werden.
- => Risiko-Analysen sind vor dem Einsatz von RFID unerlässlich.
- Eine genaue Prüfung, welcher Tags und Reader welchen Standards genügen (und welche Sicherheits-Features jetzt oder zukünftig implementieren) ist sicher hilfreich.
- Die aktuelle Markt-Dynamik nimmt auf Security wenig Rücksicht ... und dies wird sich absehbar auch nicht ändern (im Zuge des Strebens nach 5ct-Tags)...



# Offene Fragen & Diskussion



Danke für Ihre Aufmerksamkeit!



- [1] Lukas Grunwald: Kuck mal, wer da funkt, in: iX 7/2004, S. 120–121.
- [2] Helena Handschuh: Contactless Technology Security Issues, in: Information Security Bulletin April 2004, S. 95–100.
- [3] Securing Off-The-Shelf RFID systems:  
[http://www.cerias.purdue.edu/homes/crisn/courses/cs590/team9\\_rfid.pdf](http://www.cerias.purdue.edu/homes/crisn/courses/cs590/team9_rfid.pdf).
- [4] Security & Privacy in RFID Systems:  
<http://lasecwww.epfl.ch/~gavoine/rfid/>
- Allgemeiner Literaturhinweis zu Angriffstechniken:  
Dominick Baier/Enno Rey/Michael Thumann: Pen-Tests – Durch Risiko-Abschätzung IT-Sicherheit optimieren [Vieweg-Verlag, ISBN 3528058390].

