Smart Brands and Product Protection 2005

Central London, UK, Europe Mar 9, 2005

Lukas Grunwald

DN-Systems Enterprise Internet Solutions GmbH 2005

dn Systems
Enterprise
Internet
Solutions
GmbH

Agenda

What is RF-ID ?

- What is RF-ID and what are Smart-Labels
- Risks and dangers with them
- Attacks against Smart-Label systems, RF-ID systems
- Demonstration of RF-ID tags and RF-Dump in practical use
- A Future Store

dn Systems
Enterprise Internet Solutions GmbH

RF-ID

RF-ID (Radio Frequency Identification) is a mechanism to get an identification remotely from:

- your remote-control for your garage
- an access control-system for a room
- a cage in a factory
- an electronic product code attached to a wrapped item in the supermarket

dn Systems
Enterprise Internet Solutions GmbH

Smart-Labels - EPC

Smart-Labels are a special form of an RF-ID application. The tags look like normal product tags, but inside is an antenna and a small microchip. The tags have a serial number and an EEPROM with the ability to store information like the EPC (Electronic Product Code), an international unique code from the manufacturer. Now the labels have mobile communication capabilities.

EPC Type 1			
01	0000A66	00016F	000169DCD
Header	EPC Manager	Object Class	Serial Number
8 Bit	24 Bit	24 Bit	36 Bit

The ISO-Standard Smart-Labels operate on the ISM Frequency 13.56 MHz

dn Systems
Enterprise Internet Solutions GmbH

Smart-Labels - Variants

Some of the well-known cheap Smart-Labels you will find today and tomorrow in some consumer-products are:

ISO 15693	Tag-it ISO, My-d, I-Code SLI, LRI512, TempSense
ISO 14443 A	Mifare Standard(1,2), Mifare UltraLight(1,2)
ISO 14443 B	SR176(1,2)
Tag-it®	
I-Code®	

dn Systems
Enterprise Internet Solutions GmbH

Smart-Labels - Features

What the tags have in common:

- have no battery, and consume the power to operate from the electro-magnetic RF-ID reader-field
- store the information in clear-text on the EEPROM
- have memory pages
- do not have read-protection
- some have special write protection
- serial number is fixed, user-data can be modified
- support up to 1000 write cycles

dn Systems
Enterprise Internet Solutions GmbH

Smart-Labels

The labels are used by manufacturers and shipping companies to optimize their supply chain:

- easy integration at the production plant
- tracking of boxes and goods
- easy sorting of boxes and packets
- just-in-time production
- tracking of the max. temperature for sensitive good (medicine, reefer cargo)

dn Systems
Enterprise Internet Solutions GmbH

Data-Center vs. Tag

- Two different approaches: Either all the information about a product is stored in a central database, and only the native serial number of the tags is used as a key, or all relevant information is stored on the EEPROM directly in the labels.
- In the field we often find a combination of both approaches where some information is stored in the label, and some is held in a central database.

dn Systems
Enterprise Internet Solutions GmbH

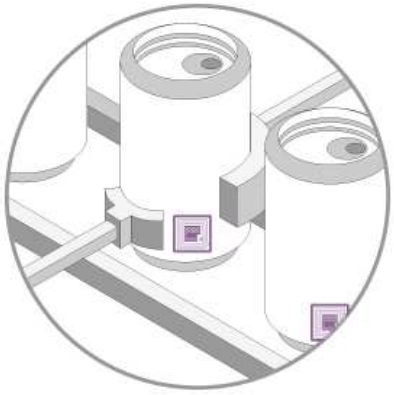
POS Benefits

Benefits of Smart-Labels at the Point of Sale:

- auto-inventory
- detect misplaced products at the shelf
- alerting the clerk to replace missing or expired goods
- track the behavior of the customer in the shop
- auto-checkout for the customer, only put the goods in your shopping bag
- the register is a RF-ID Gate, you only need to use your credit-card or have your RF-ID customer card with you to make a quick checkout

dn Systems
Enterprise Internet Solutions GmbH

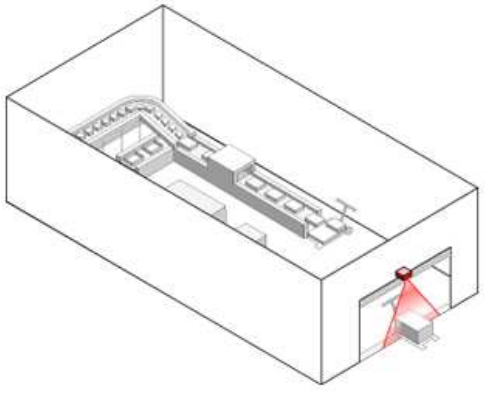
Brave New Supply Chain 1



- At production time, the Smart-Label is placed on the product

dn Systems
Enterprise Internet Solutions GmbH

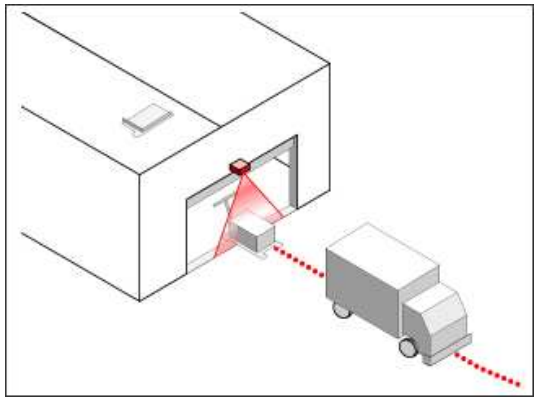
Brave New Supply Chain 2



- Each product is registered inside its package when leaving the factory
- Here, the EPC is written to the ID-Tags

dn Systems
Enterprise Internet Solutions GmbH

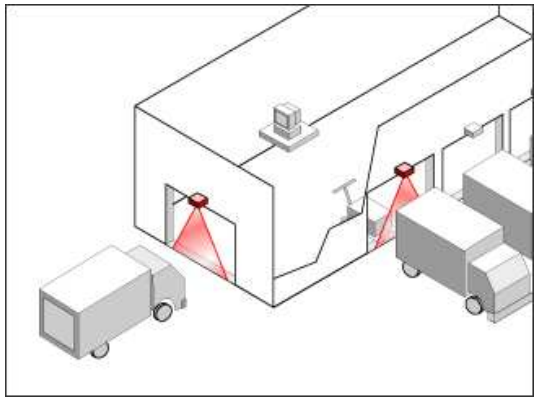
Brave New Supply Chain 3



- If a customer orders the product through a reseller, the palettes are tracked on their way

dn Systems
Enterprise Internet Solutions GmbH

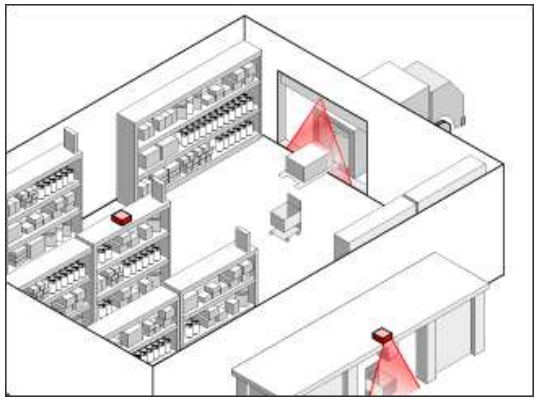
Brave New Supply Chain 4



- At the reseller site, the new goods are registered upon arrival
- Temperature and expiration date can be checked at delivery time

dn Systems
Enterprise Internet Solutions GmbH

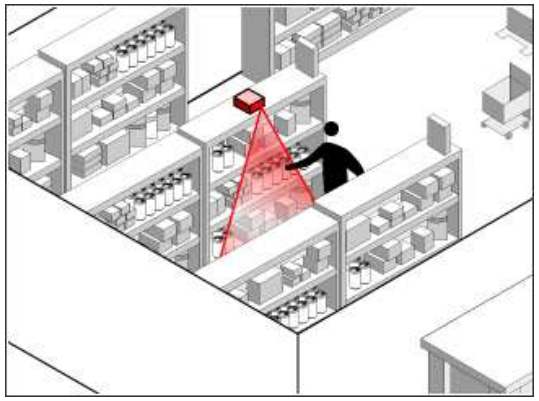
Brave New Supply Chain 5



- The palette arrives at the store, all products entering the store are registered by the entry gate

dn Systems
Enterprise Internet Solutions GmbH

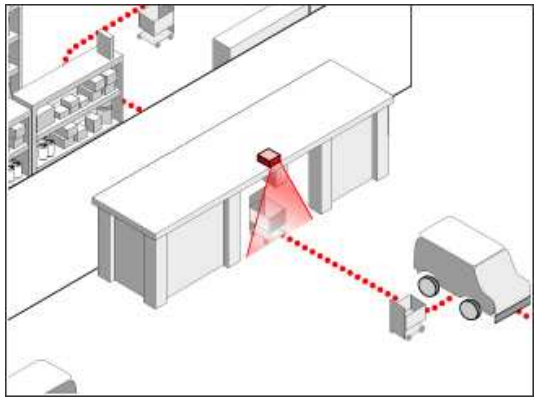
Brave New Supply Chain 6



- In the store the customer takes a retail-package, the RF-ID reader in the shelf detects this
- If the shelf runs out of products or detects a misplaced product it can escalate this information to the clerk in the shop

dn Systems
Enterprise Internet Solutions GmbH

Brave New Supply Chain 7



- The customer leaves the store, the register reads the RF-ID tag from inside the customer's shopping-bag
- Fast self-checkout and shop-lifting prevention at the same time

dn Systems
Enterprise Internet Solutions GmbH

Smart White Goods

Benefits for consumers could emerge from the intelligence of domestic appliances:

- Smart fridge
  - Auto-inventory
  - Expiration management of goods
- Intelligent washing machine
  - Automatic choice of correct program
  - Detecting red socks among white undies

dn Systems
Enterprise Internet Solutions GmbH

Myths and Facts about RF-ID

- Myth:

RF-ID tags have the size of a pin and can be embedded into any product.

- Fact:

This is not true, the electro-magnetic fields have problems with metal and other shielding material. You also need an antenna to connect the RF-ID chip to the field, the antenna has some minimum size requirements.

dn Systems
Enterprise Internet Solutions GmbH

Myths and Facts about RF-ID

- Myth:

RF-ID chips can be read from a huge distance.

- Fact:

This is not true, you must be in a field to power the chip via the antenna, the maximum distance from a strong gate is around 10 meters.

dn Systems
Enterprise Internet Solutions GmbH

Public Information

RF-ID tags can be read by everyone! You need:

- RF-ID Reader, we use the Multi-Tag Reader from ACG Germany
- An antenna or a gate to build the field
- Tags
- A PC or laptop to process the information from the reader
- Our tool to process the information

dn Systems
Enterprise Internet Solutions GmbH

ISO 15693 Tags

- Each tag has an unique identifier (UID)
- UID is required for anti-collision algorithm if more than one tag is in the field
- UID is factory-programmed and can't be changed
- The tag memory is partitioned into two blocks
  - Administrative Block containing
    - unique identifier (UID)
    - application family identifier (AFI)
    - data storage format identifier (DSFID)
- User Data
  - stores up to 128 bytes of arbitrary user data persistently

dn Systems
Enterprise Internet Solutions GmbH

RF-Dump

- tool to read and write ISO tags and Smart-Labels by Boris Wolf and Lukas Grunwald
- supports and detects nearly all Smart-Labels
- requires an ACG Compact-Flash RF-ID Reader
- runs on PDA and notebook
- Free-Software (GPL) http://www.rf-dump.org

dn Systems
Enterprise Internet Solutions GmbH

Attacks against Smart-Labels

- Most Smart-Labels are not write-protected
- The UID and Administrative Block can’t store the EPC
- EPC is stored in the User Data Area
- Meta-data like "best-before" are also stored in the User Data Area
- It’s only a matter of time until everybody will wear at least one RF-ID tag

dn Systems
Enterprise Internet Solutions GmbH

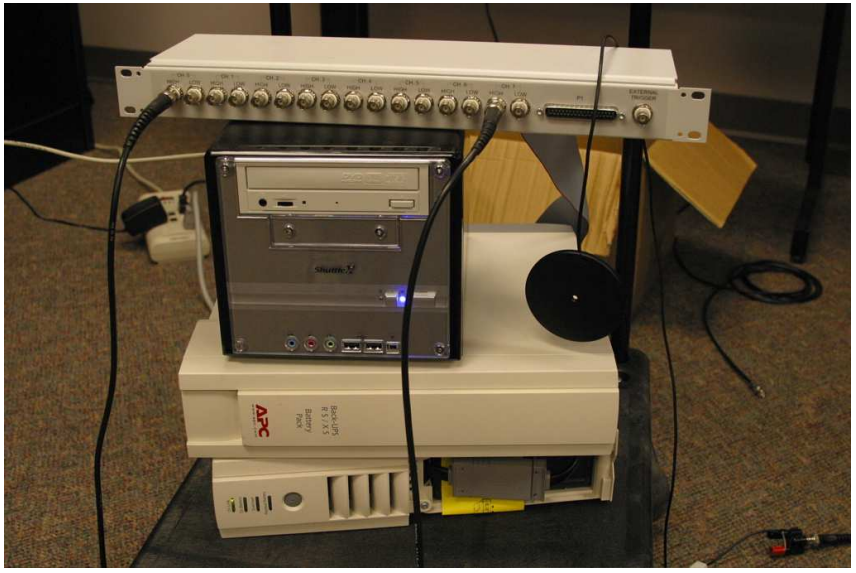
Encryption - A Solution?

- Texas Instruments DST RFID
  - Uses a proprietary cipher with a 40-bit key
  - Used in more than 150 million vehicles
- Broken with classical crypto-analysis methods
- Even with encrypted EPC-Tags you can guess with million of used tags
- Do not use symmetric algorithms!
- Asymmetric cryptography requires a huge key-space (2048 bit)
- Keep up to date with new computing-power and Moore's Law

dn Systems
Enterprise Internet Solutions GmbH

Encryption - A Solution?

A TI DST RF-ID key



System to break it

dn Systems
Enterprise Internet Solutions GmbH

Privacy Problems

- Gates can be installed anywhere
- Competitors can read what type of undies you wear, and what else you have in your shopping bag
- Big Brother can read what type of books you read
- Together with a passport or customer-card with RF-ID chip this technology poses an even bigger risk
- The customer is traceable for everyone

dn Systems
Enterprise Internet Solutions GmbH

Environmental Pollution

- If every retail packet has a RF-ID chip, there will be a significant environmental pollution issue
- The transponder or tag itself contains some harmful substances
- Non-ionizing radiation, there are some voices that say it could be unhealthy

dn Systems
Enterprise Internet Solutions GmbH

Technology Problems

- Dependency on a new technology introduces new risks
- Attacks against the RF-ID infrastructure can push companies out of business
- New possible breach for terrorist attacks and new critical infrastructure

dn Systems
Enterprise Internet Solutions GmbH

Real-Life Cookie

- As on Web-Sites you can put a real-life cookie on someone who wears clothes with Smart-Labels or carries an item containing a tag.
  - Every time he passes your gate or RF-ID field e.g. in front of your shop window you increment it by one
  - The next time you get his credit-card number, you can write his tag with a clear ID, you know who was looking at your shop window
  - You can also check if the customer takes a product out of the shelf and puts it back, so if he is unsure, you can make an instant discount only for him in 10 sec.

dn Systems
Enterprise Internet Solutions GmbH

The Future-Store

- Initiated by the Metro Corporation and several technology partners
- First store using RF-ID technology at customer shelves
- Uses RF-ID technology for age-control of X-rated movies
- Uses RF-ID technology for every palette in stock
- Puts ISO-Tags also in customer cards.
- After immense protests from privacy organizations offered a RF-ID de-activator

dn Systems
Enterprise Internet Solutions GmbH

The Future-Store

dn Systems
Enterprise
Internet
Solutions
GmbH

The Future-Store

- Customer can use a PSA (Personal Shopping Assistant) and check every product placed in the shopping cart
- Customer can also do a self-checkout
- Customer is guinea pig for new technology
- Perfect area for our first field-test of RF-Dump

dn Systems
Enterprise Internet Solutions GmbH

Future-Store Testfield

dn Systems
Enterprise
Internet
Solutions
GmbH

The RFID-Deactivator

- After checkout Metro offers a "RFID-Deactivator" for the customer
- In fact, it overwrites the User Data Area with zeros
- Tag can be rewritten after the de-activation
- Serial-ID and Administrative Block can’t be erased
- At the exit-gate the tag can be instantly filled with other information
- To use the Deactivator all User Data Areas MUST be writable in the shop, which offers a lot of options for new attacks and fun in the store.

dn Systems
Enterprise Internet Solutions GmbH

Future-Store Testfield

dn Systems
Enterprise
Internet
Solutions
GmbH

Chaos in the Future-Store

- You can convert the EPC from cream cheese into shampoo, the store computer believes your cream cheese is misplaced in this shelf
- Put the cream cheese after converting in the shampoo shelf
- Make some X-rated movies G-rated, now kids can buy them with the Self-Checkout
- Convert your favorite new DVD into the one on sale for 5 Euro

dn Systems
Enterprise Internet Solutions GmbH

Further Attacks

- Most software is written without security in mind, at least supply chain software: Possible exploits via manipulated data fields in the User Data Area
- Some registers make an instant reboot after reading a RF-ID tag with manipulated fields
- If you shield the field, no EAS or RF-ID system can possibly read a tag, a simple aluminum-foil-wrap is sufficient

dn Systems
Enterprise Internet Solutions GmbH

Risks for the Companies

- Whole new area of shop-lifting
- Chaos and attacks are possible
- Customers can change the EPC and no one will detect it when using self-checkout
- Attacks can also be used on medical drugs and age-restricted material
- Attackers only need a publicly available RF-ID Reader/Writer

dn Systems
Enterprise Internet Solutions GmbH

That's it...

THANK YOU !

Questions?

email:

l.grunwald@dn-systems.de

dn Systems
Enterprise
Internet
Solutions
GmbH