3rd European Workshop on RFID Systems and Technologies
12./13. June 2007, Duisburg

Security challenges for RFID key applications

Ulrich Waldmann
Fraunhofer-Institut SIT

TZi Technologie-Zentrum Informatik

MES

SIT
Fraunhofer Institut
Sichere Informations-
Technologie

Content

- Discussion of product anti-counterfeiting with RFID

- Background
- Pharmaceutical supply chain with RFID
  - Motivation to introduce RFID
  - Implementation example
    - Achieved security level
    - Attack scenario
  - Recommended security solution
  - Summary

Background: RFID security report

"Technology-integrated data security of RFID systems" (in German only)

- Application-specific security requirements
- Recommended security measures
- Open R & D issues

TZi Technologie-Zentrum Informatik MES Fraunhofer SIT Institut Sichere Informations-Technologie

Technologieintegrierte Datensicherheit bei RFID-Systemen

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Three RFID application scenarios:

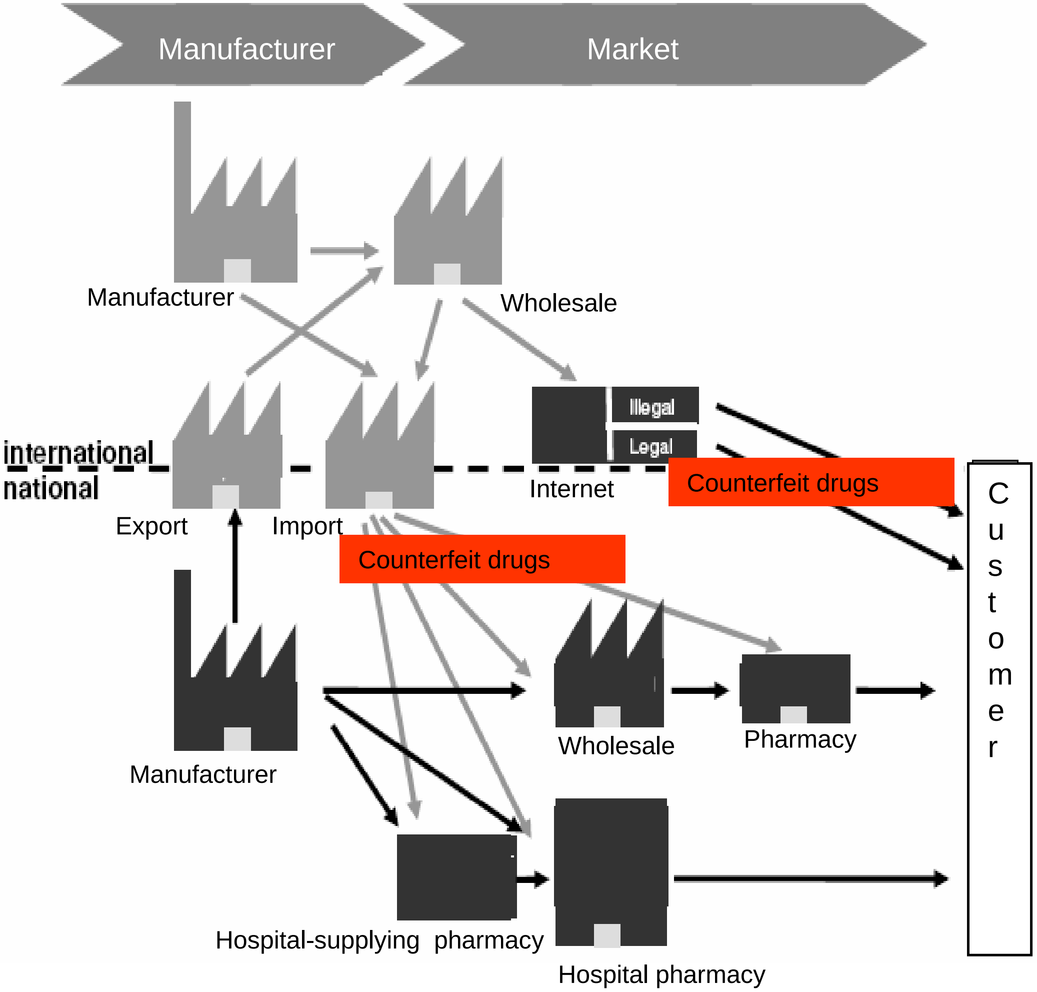
1. **Automotive production**: Identification of components
2. **Retail supply chains**: Identification of consumer goods
3. **Pharmaceutical supply chain**: Drug anti-counterfeiting

Free download: www.sit.fraunhofer.de/rfid-studie2007

Pharmaceutical supply chain with RFID: motivation

WHO: 5-8% of global drug turnover by counterfeit products

- US Food & Drug Administration (FDA)
  - ➢ RFID on item-level recommended
  - ➢ Electronic pedigree
- RFID concepts of EPCglobal most promising
  - ➢ Electronic Product Code (EPC)
- European wholesalers against RFID
  - ➢ Pushing of 2-dim. Barcode (EAN 128)
  - ➢ Specific national requirements (e.g. PZN)
  - ➢ RFID too expensive and not reliable
  - ➢ EPC needs network & databases
  - ➢ EPC without batch number, expiring date

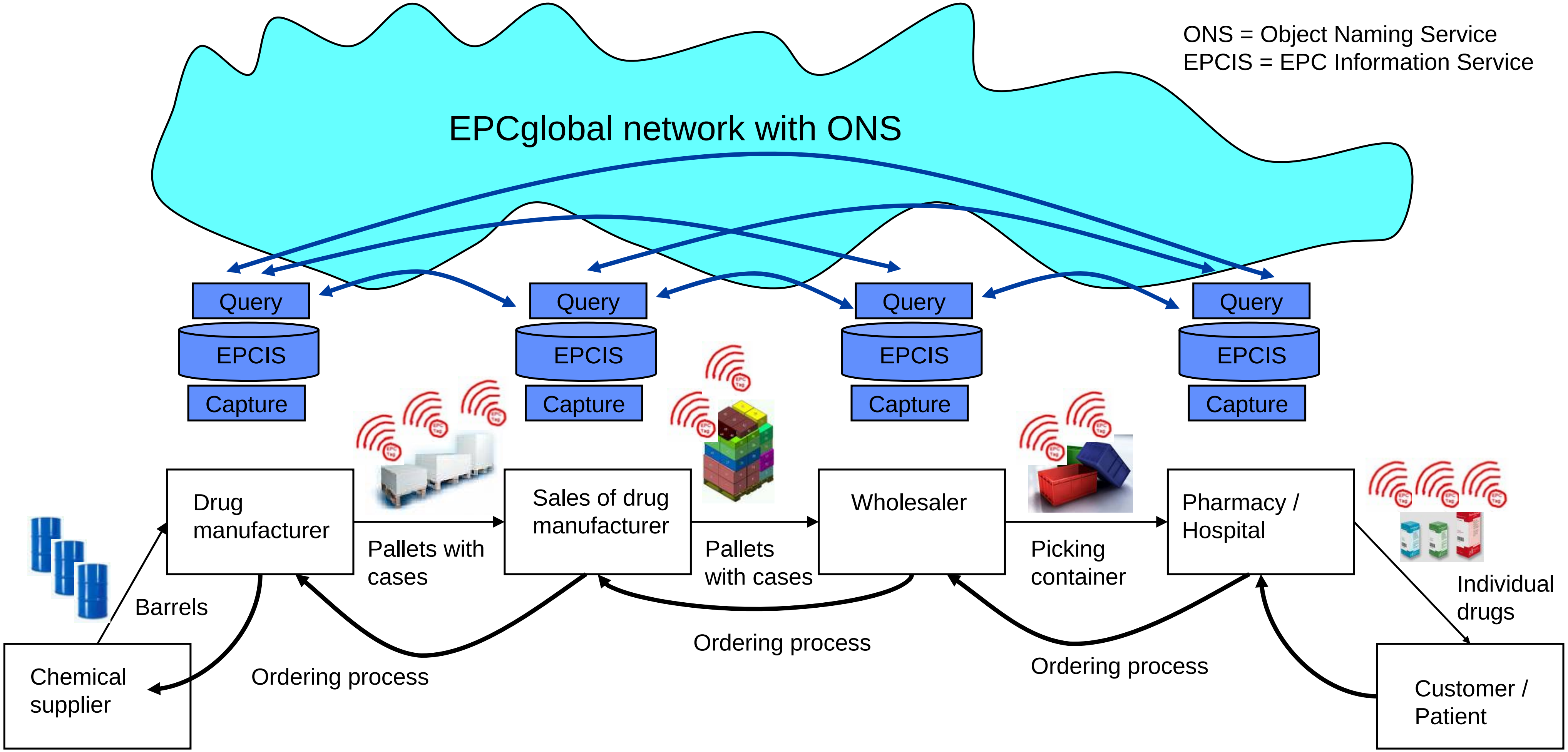


Source: [platzen06]

Existing RFID solution (IBM, USA)

Major objectives: Proof of genuineness of traded drugs, tracking & tracing

ONS = Object Naming Service
EPCIS = EPC Information Service



Characteristics of the RFID solution (IBM, USA)

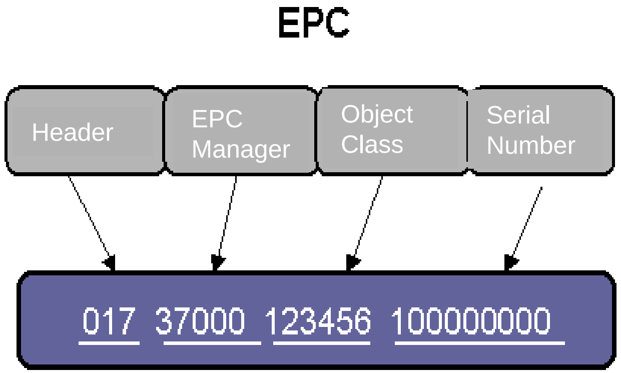
Minimal data on passive EPCglobal tags

- Tag ID from chip manufacturer: „burnt-in code“ with chip serial number
- EPC from drug manufacturer with serial number of product
- Drug manufacturer registers product under both identifiers

Tag ID

with serial number

+



Proof of origin and drug genuineness

- Access to EPCIS via XML queries over EPCglobal network
- If product not registered: probably counterfeit
- Duplicate check using the combination of tag ID / EPC
- The parts of the pedigree remain at their original EPCIS

Anti-counterfeiting is based on assumption that “burnt-in“ tag identifier can not be copied

Security considerations

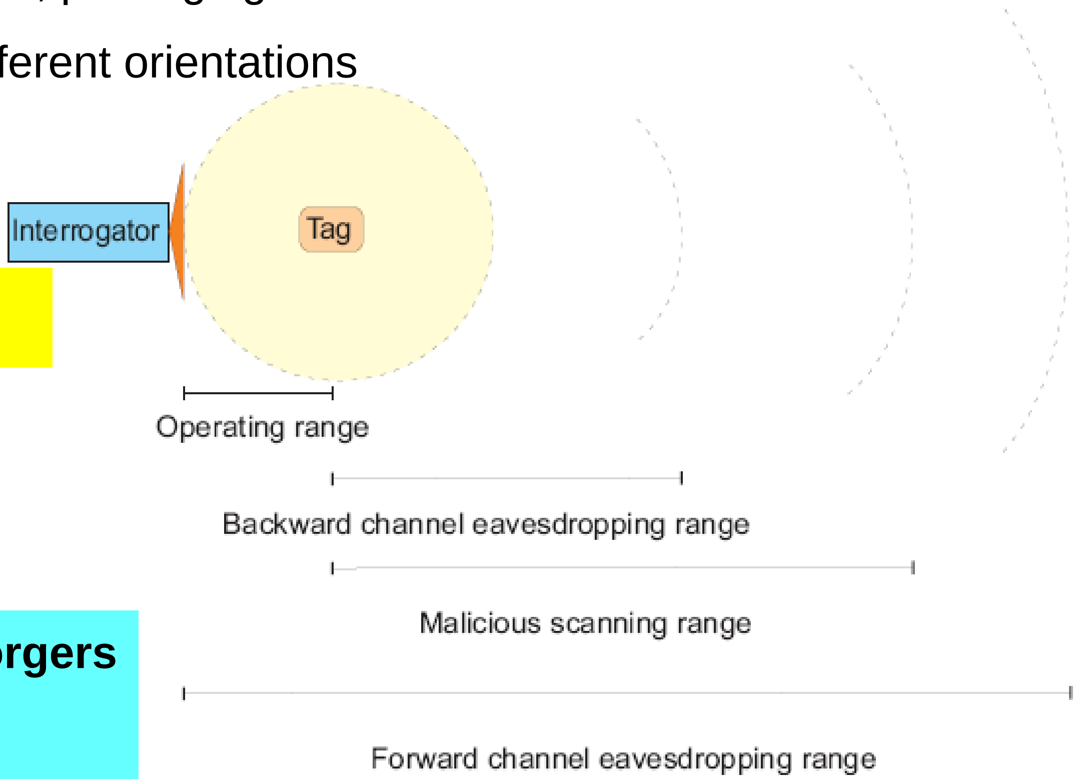
Functional reliability takes priority over security mechanisms

- Customers consider that verification of identifiers is effective
- Most discussions about choice of HF or UHF on item level
  - ➢ Heterogenous reading conditions, materials, packaging
  - ➢ High line-speeds, dense aggregations, different orientations
  - ➢ 100% reading rate not reached

But: attacks at the RFID air interface possible

- Unauthorized reading of tag data (sniffing)
- Tag cloning

Sniffing and tag cloning may be used by forgers to label counterfeit products


Interrogator
Tag
Operating range
Backward channel eavesdropping range
Malicious scanning range
Forward channel eavesdropping range

Source: [ranasinghe06]

Example of an attack scenario

Counterfeit drugs with cloned RFID tags

- **Problems**
  - Current EPC tags (CLASS1 Gen2) are passive low-cost tags
  - No overall security concept
  - Unrestricted reading access to tag data (Tag ID, EPC)
  - Counterfeiters may have access to freely programmable tags
  - Unsecured tag connection with product

- **Proposed security solution**
  - **Security level 1:** Verification of tag identifiers
  - **Security level 2:** Verification by means of electronic pedigree
  - **Security level 3:** Verification by means of cryptographic tag authentication
  - **Security level 4:** Verification of the product (correlation tag -> product)

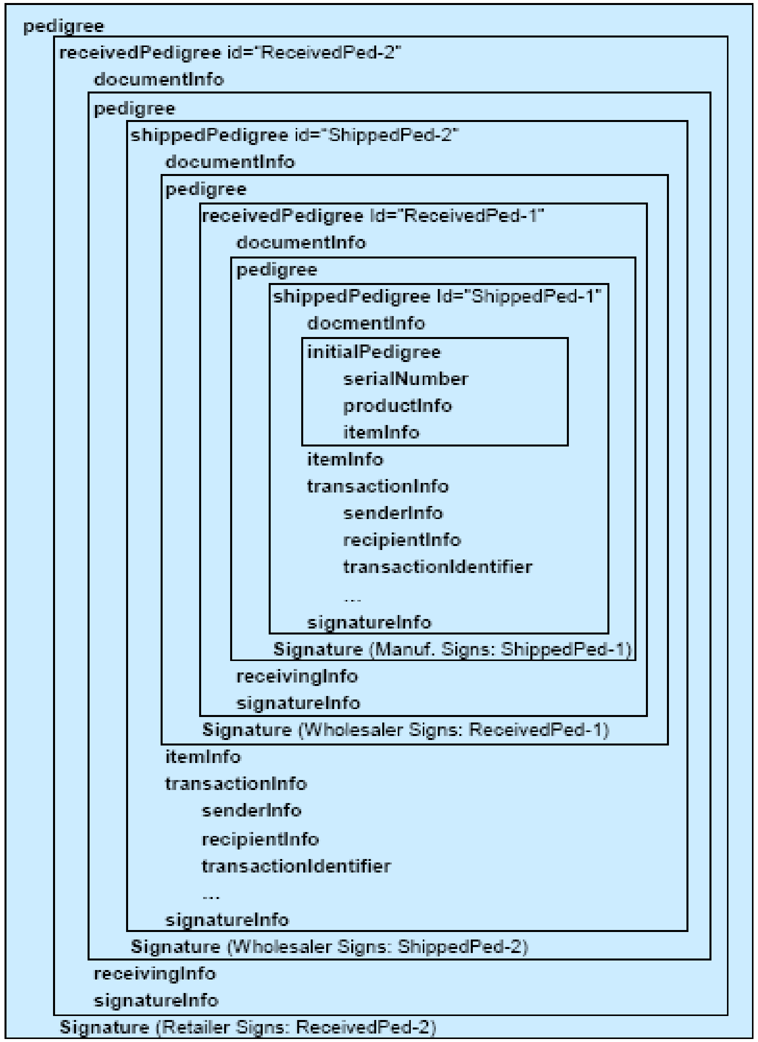
Security level 1: Tag identifiers and level 2: Electronic pedigree

Read-only tag identifiers available on EPC tags

- Tag serial number stored by chip manufacturer
- Product serial number stored by drug manufacturer
- Valid combinations registered with drug manufacturer

Electronic pedigree according to EPCglobal

- Each receiving party adds information and digitally signs the whole document
- Whole pedigree sent along with product
- Plausibility tests with product & transaction info
- Possible to append files (e.g. product images)



```
pedigree
  receivedPedigree id="ReceivedPed-2"
    documentInfo
    pedigree
      shippedPedigree id="ShippedPed-2"
        documentInfo
        pedigree
          receivedPedigree Id="ReceivedPed-1"
            documentInfo
            pedigree
              shippedPedigree Id="ShippedPed-1"
                docmentInfo
                initialPedigree
                  serialNumber
                  productInfo
                  itemInfo
                itemInfo
                transactionInfo
                  senderInfo
                  recipientInfo
                  transactionIdentifier
                  ...
                signatureInfo
              Signature (Manuf. Signs: ShippedPed-1)
            receivingInfo
            signatureInfo
          Signature (Wholesaler Signs: ReceivedPed-1)
        itemInfo
        transactionInfo
          senderInfo
          recipientInfo
          transactionIdentifier
          ...
        signatureInfo
      Signature (Wholesaler Signs: ShippedPed-2)
    receivingInfo
    signatureInfo
  Signature (Retailer Signs: ReceivedPed-2)
```

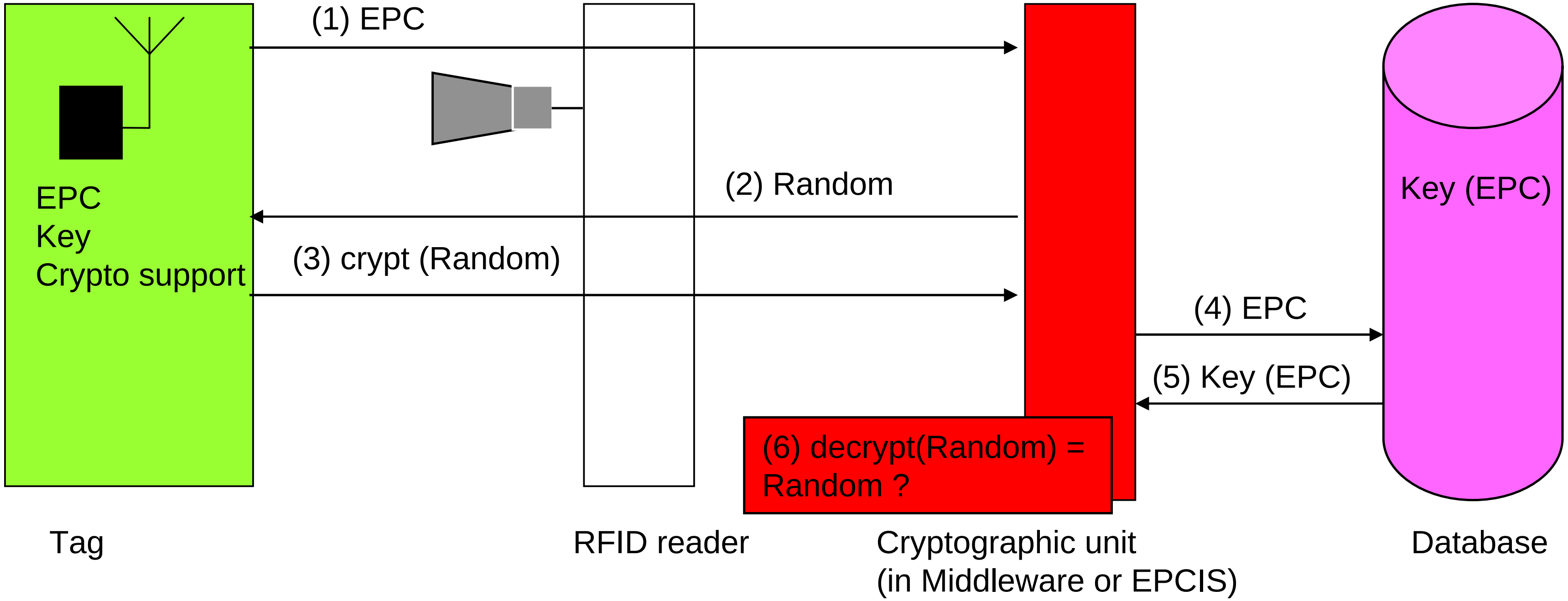
Pedigree not sufficient against counterfeiting:

Counterfeit products may refer to valid pedigrees

Solution level 3: Tag authentication

Strong authentication with challenge-response using tag-individual keys

- Would be best solution from the security point of view
- Though impractical in open supply chains with unknown set of tags



Strong authentication hardly feasible on low-cost tags: no cryptographic unit on tag real-time requirements, complex key management, database access

Solution level 3: Tag authentication (cont.)

Restrictions on low-cost tags

- Number of electronic gates only 5.000 to 10.000
- Maximum 2.000 available for security

RSA (1024 bit):	67.000
AES (128 bit):	20.000-30.000
Lightweight ECC (163 bit):	15.094
Lightweight AES (128 bit)**:**	3.595
Lightweight DES (112 bit):	2.168

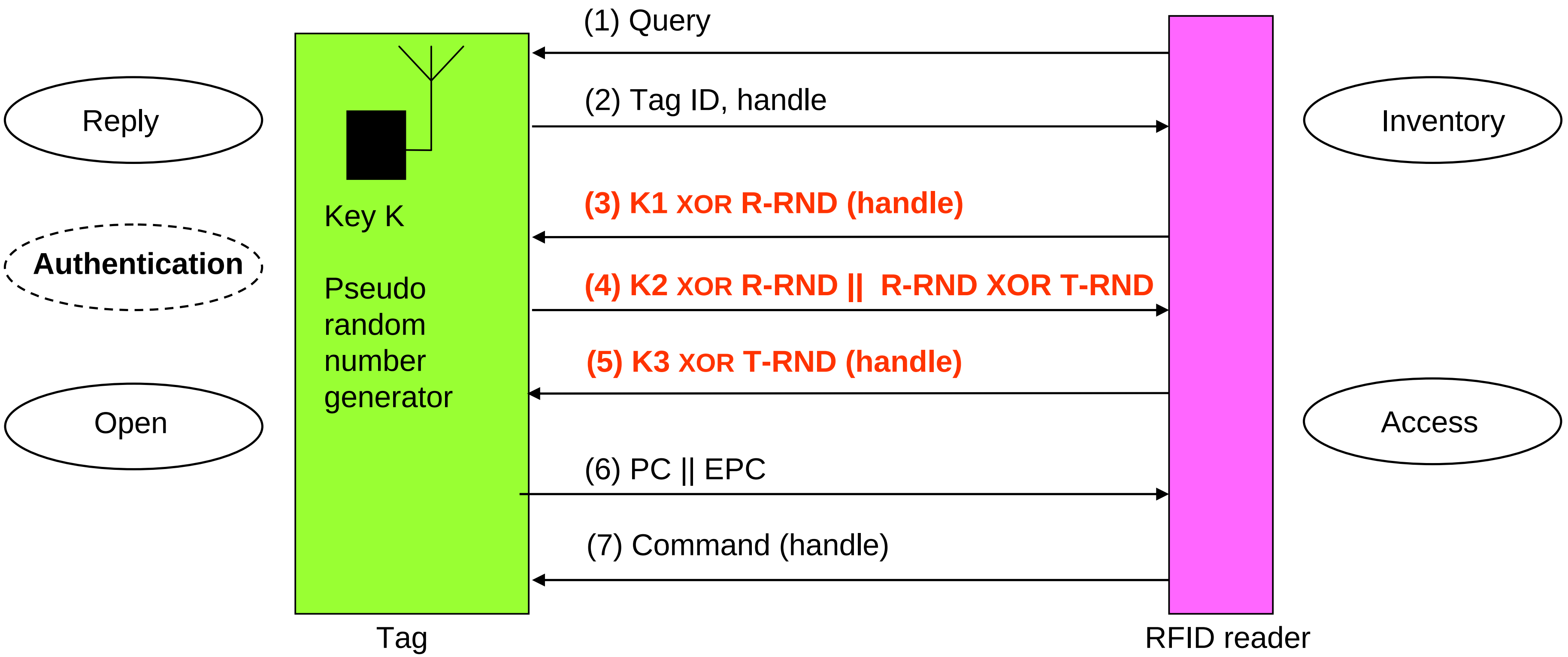
- Legal regulations on frequencies, bandwidths etc.
- Limited power supply
- Frequent power interruptions
- Tags are not tamper-resistant

Restricted cryptography due to hardware limits, desired overall performance & costs

Solution level 3: Tag authentication (cont.)

Search for cryptographic operations that go with low-cost tags

- Example of lightweight authentication: simple bit operations (XOR) with subkeys K1, K2, K3



Efficient operations on tag, but complex in terms of key distribution: database access, synchronization, security of keys?

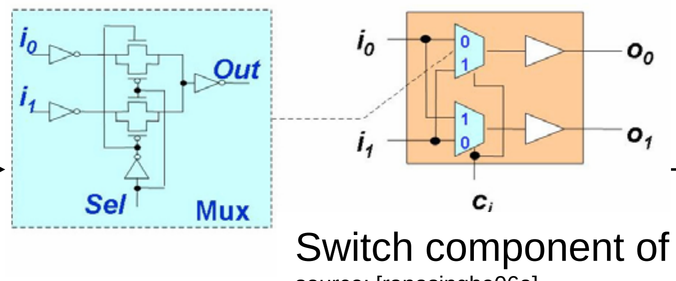
Solution level 3: Tag authentication (cont.)

Replace permanent cryptographic keys by something else, e.g.

- **One-Time Codes**
  - Simple XOR encryption and decryption
  - Very secure mechanism, if code is truly random, secret and used only once
  - Research: generation, synchronization

- **Physical Uncloneable Functions (PUFs)**
  - Uncontrollable differences during chip manufacturing
  - Characteristic response to a certain input (like secret key operation)
  - Storage of challenge-response pairs on server
  - Research: voltage effects, suitable protocols

challenge, e.g. **001101001** →



→ response, e.g. **100101100**

Switch component of PUF

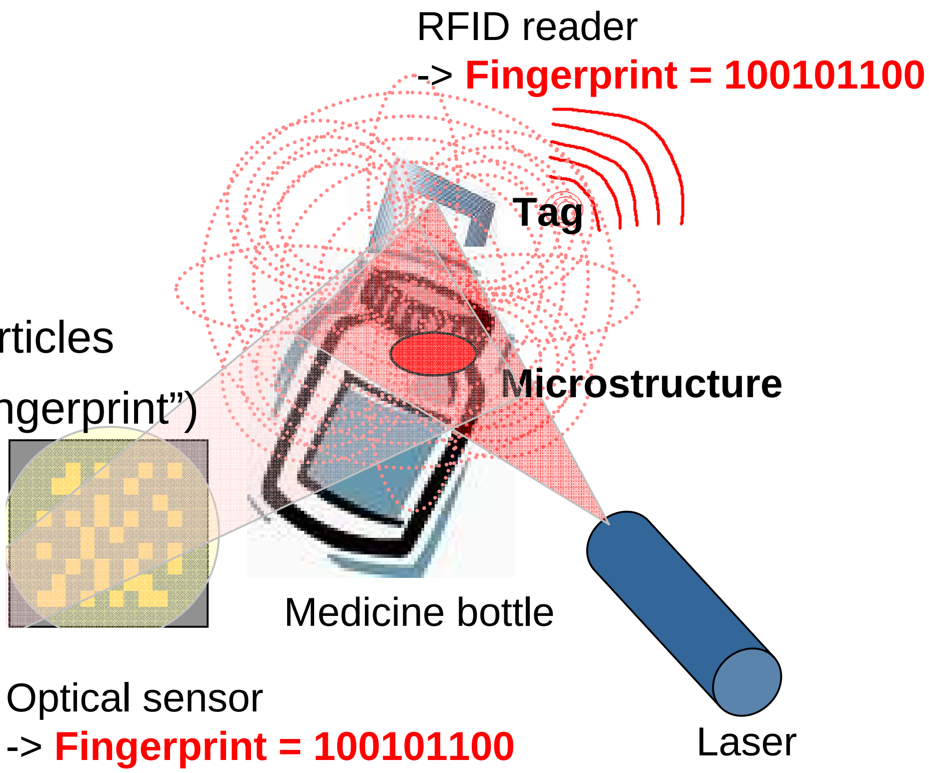
source: [ranasinghe06a]

One-Time Codes and physical fingerprints are promising approaches (long-term)

Solution level 4: Product authentication

Alternatives to static features on packaging (hologram, watermark, special design)

- **Verifiable connection of tag with product e.g.**
  - Signed tag data also printed on packaging
  - Optical features of packaging shown in pedigree
  - Tag inlays of sealed bottles
- **Physical One-Way Functions (POWFs)**
  - 3-dim. microstructure with randomly embedded particles
  - Unique interference pattern -> unique bit string (“fingerprint”)
  - Verification of the fingerprint (also stored on tag)



Step 1: Tag authentication

Step 2: Reading fingerprint from tag memory

Step 3: Detecting fingerprint from microstructure

Step 4: Detected fingerprint = read fingerprint?

Summary

- Pharmaceutical industry could be the first to introduce RFID on item-level
- Drug anti-counterfeiting is a promising RFID application scenario
- Current solutions with tag identifiers & pedigree
- New methods of tag and product authentication needed
- Physical fingerprints may complete solutions against counterfeiting in the long term

Thank you!

18. SIT SmartCard Workshop
5./6. February 2008

Ulrich Waldmann
Rheinstr. 75
64295 Darmstadt
Phone: 06151-869-222
Mail: ulrich.waldmann@sit.fraunhofer.de

SIT

Fraunhofer Institut
Sichere Informations-
Technologie