RFID Security and Privacy

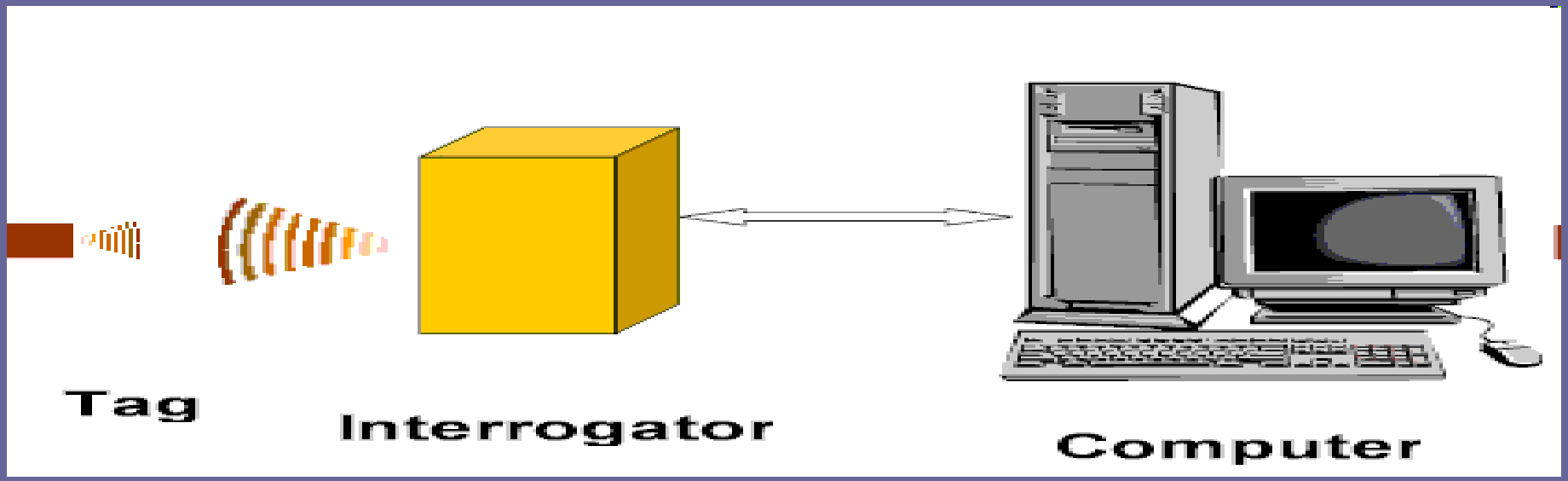
Mainly based on “RFID Security and Privacy: A Research Survey” by Ari Juels, RSA Laboratories, 28 September 2005

What is RFID?

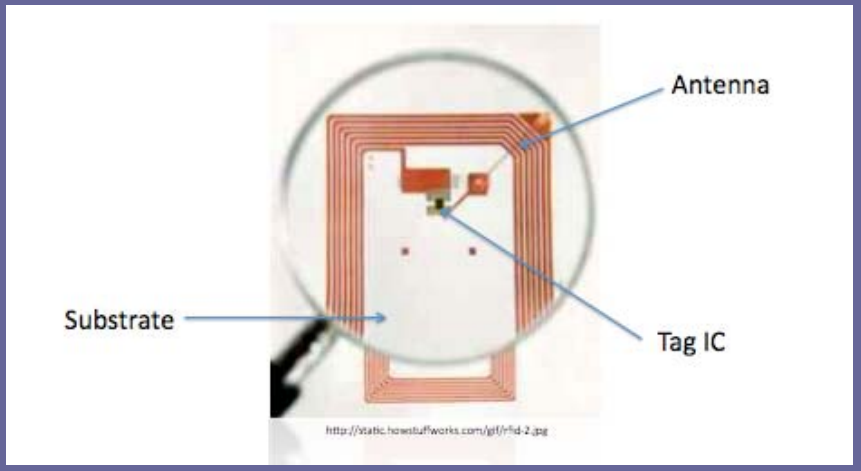
- Radio Frequency IDentification
- Small, wireless devices
- Main function: identification of an object or person
- Facilitate the acquisition and storage of data

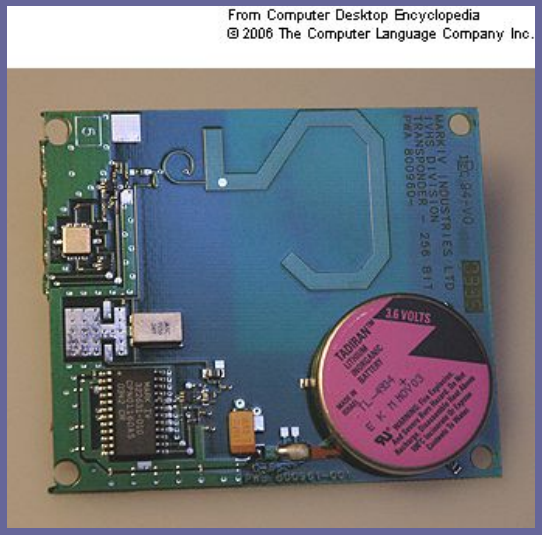
RFID – System

- Transponder placed on or within the object or person
- Reading device for reading the transponder ID



Different kinds of RFID tags





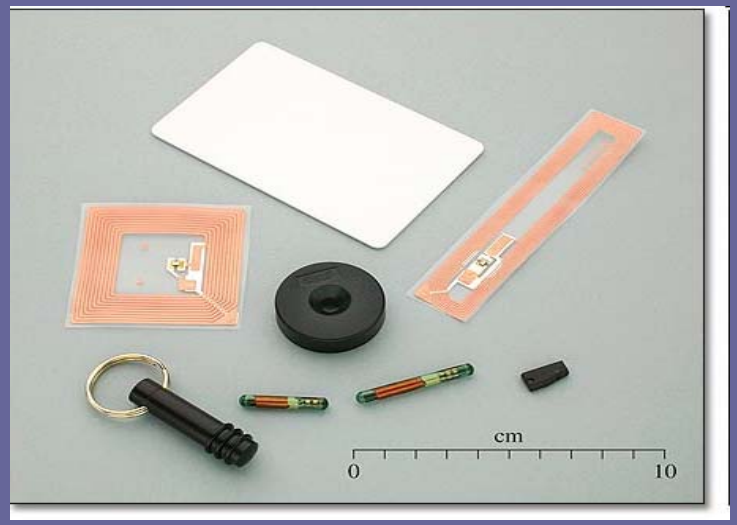
- **Passive tags (Basic RFID tags)**
- Small and inexpensive
- No on-board power source
- Transmission power from reader
- Just readable, you can't write anything on them

- **Semi-passive tags**
- Contain batteries
- Batteries only in use when interrogation by reader

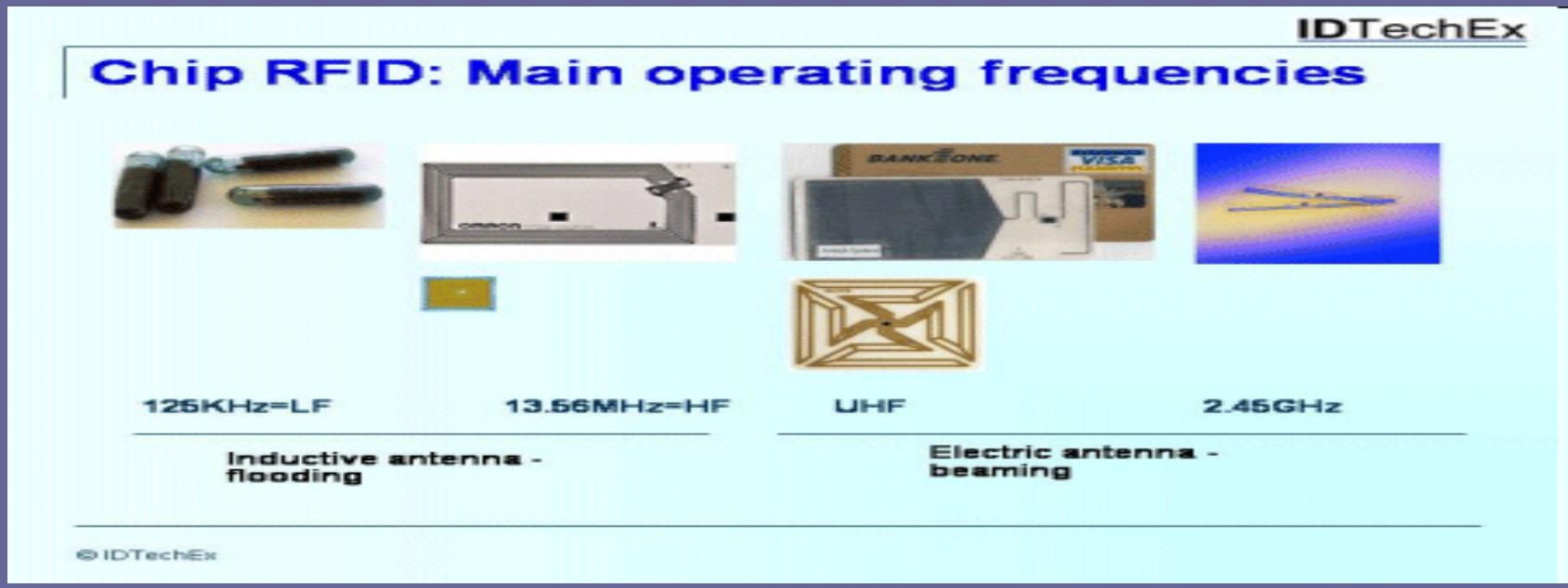
Different kinds of RFID tags

- **Active tags**
- Batteries power their transmissions
- Can initiate communication
- Read ranges of 100m or more
- Much more memory capacity, writeable

Different kinds of RFID tags



- RFID tags can take many different forms
- RFIDs use different frequencies (e.g. LF, HF and UHF tags)

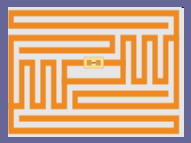


RFID Today

Sample Applications

RFID – Successor to the barcode

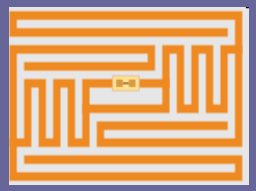
- Identification of the object
- Optically scanned, require line-of-sight contact with readers



- unique identification, emits a unique serial number
- unique identifiers can act as a pointer to a database
- readable without line-of-sight contact
- RFID readers can scan tags at rates of hundreds per second

EPC (Electronic Product Code)

- Main form of barcode-type RFID device
- 0.05$ per tag
- Little data in on-board memory
- EPC code up to 96 bits in length
- Pointer to database records
- ONS (Object Name Service)

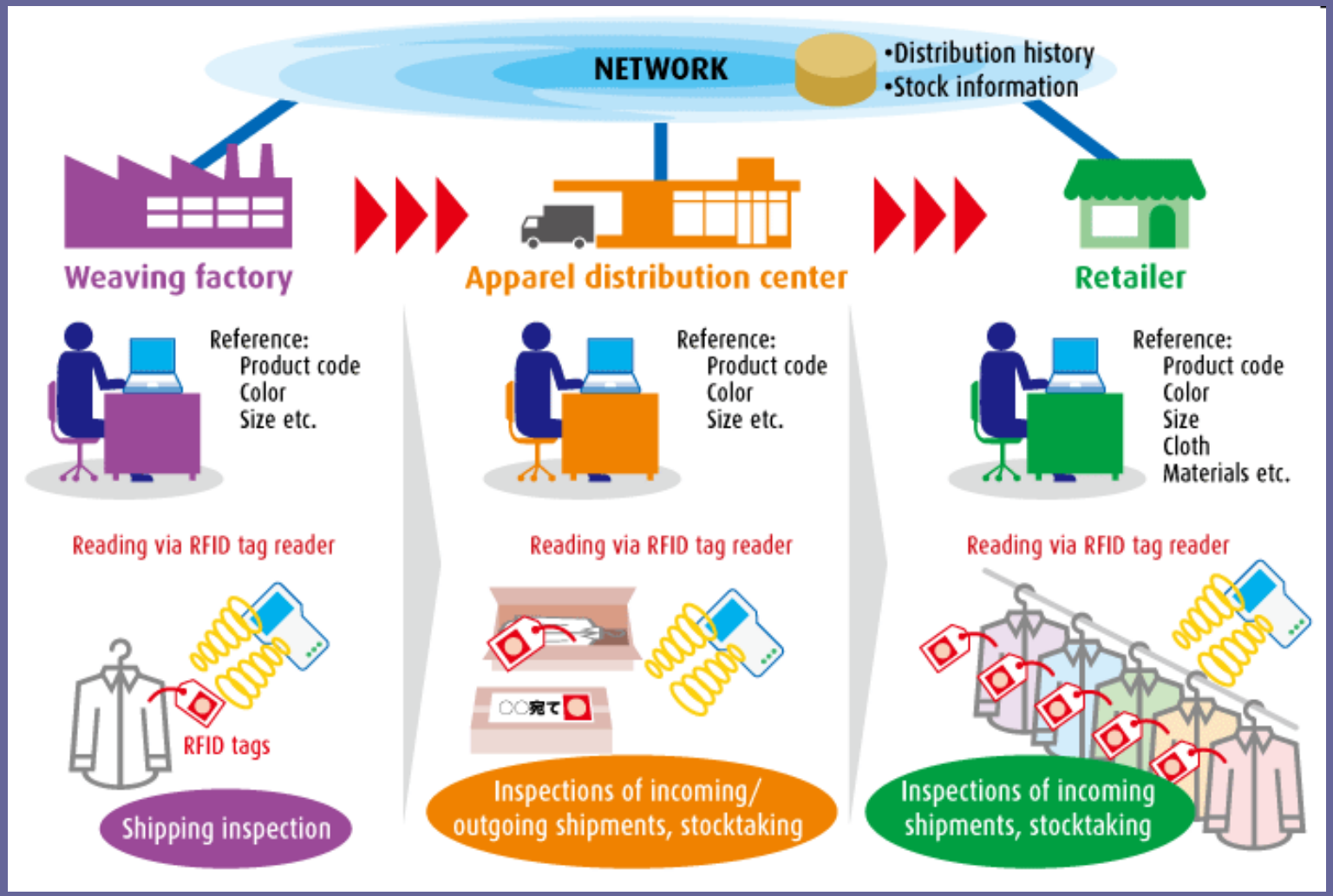


RFID tagging of goods

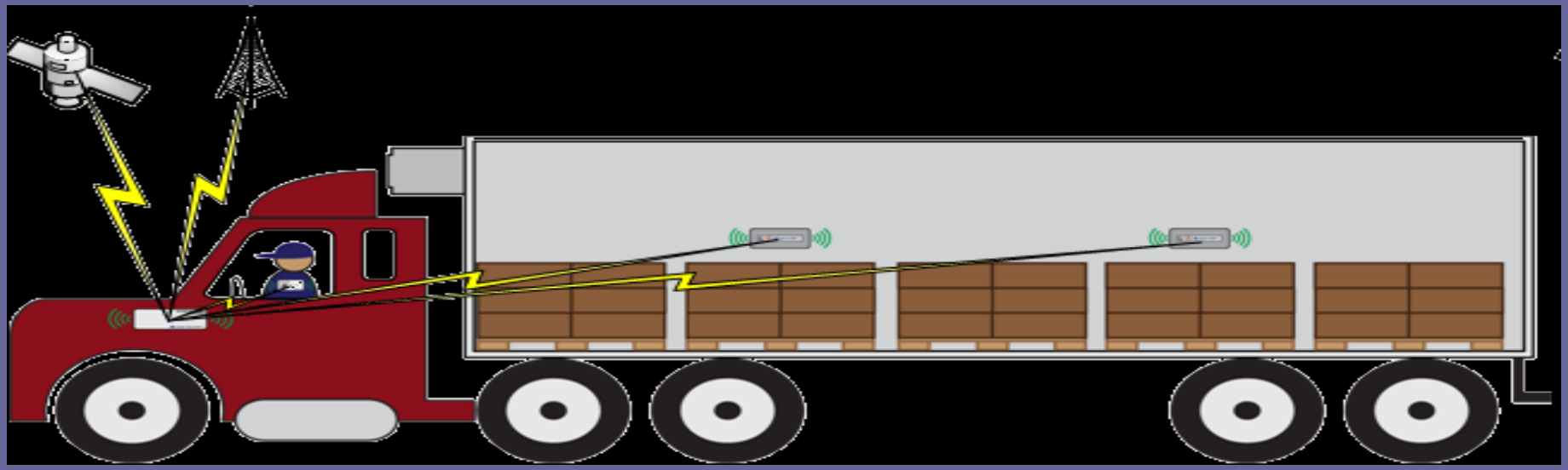
- RFID tagging of crates and pallets
- Improved accuracy and timeliness of information about the movement of goods in supply chains

Automated oversight supply chains

Better supply-chain-visibility



Food transportation



- RFID tag connected to sensor to save measured data like temperature, humidity or vibrations
- Used for proof of compliance with cold chains of food transportations

Proximity cards

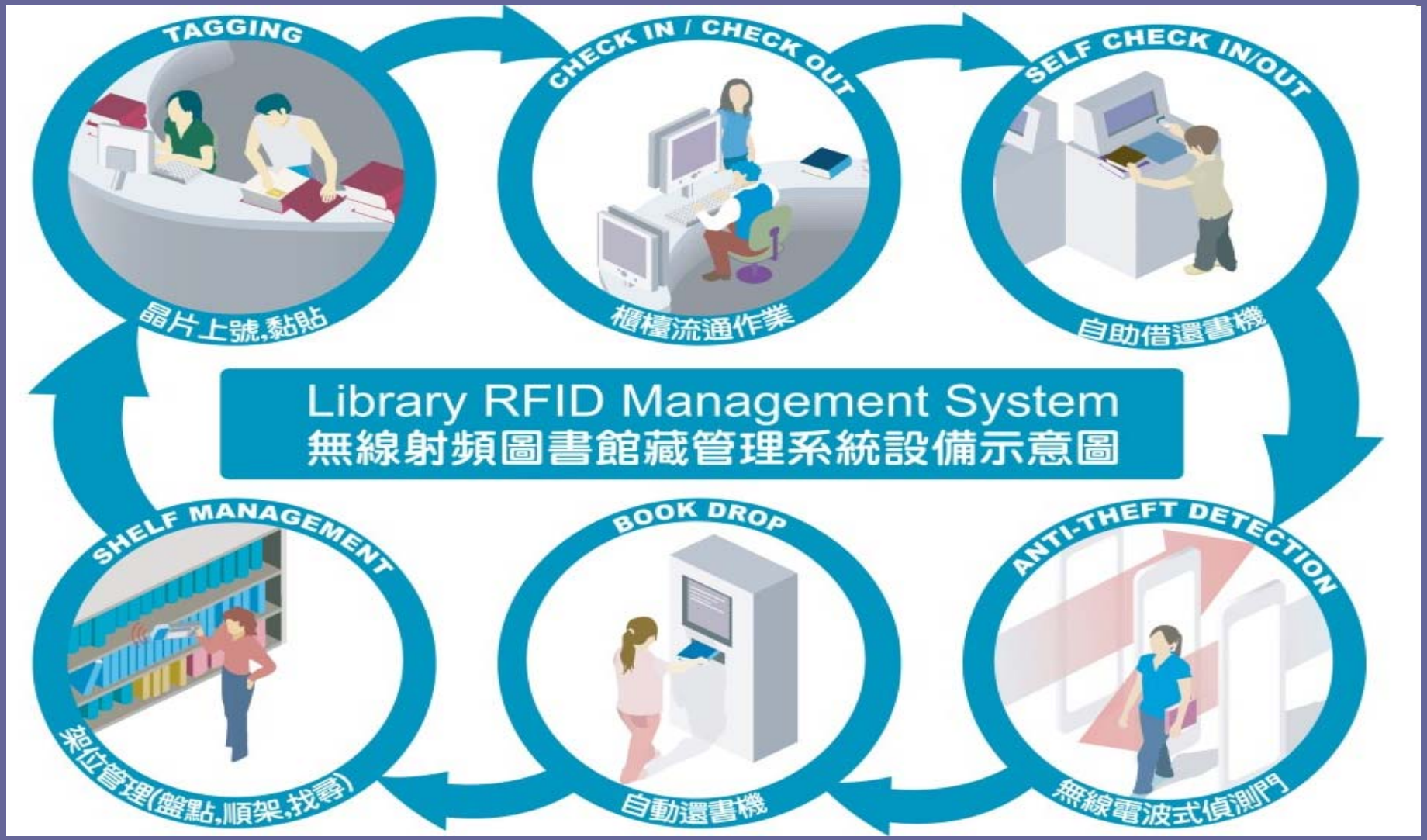
Ignition key

RFID tags protect millions of cars against theft

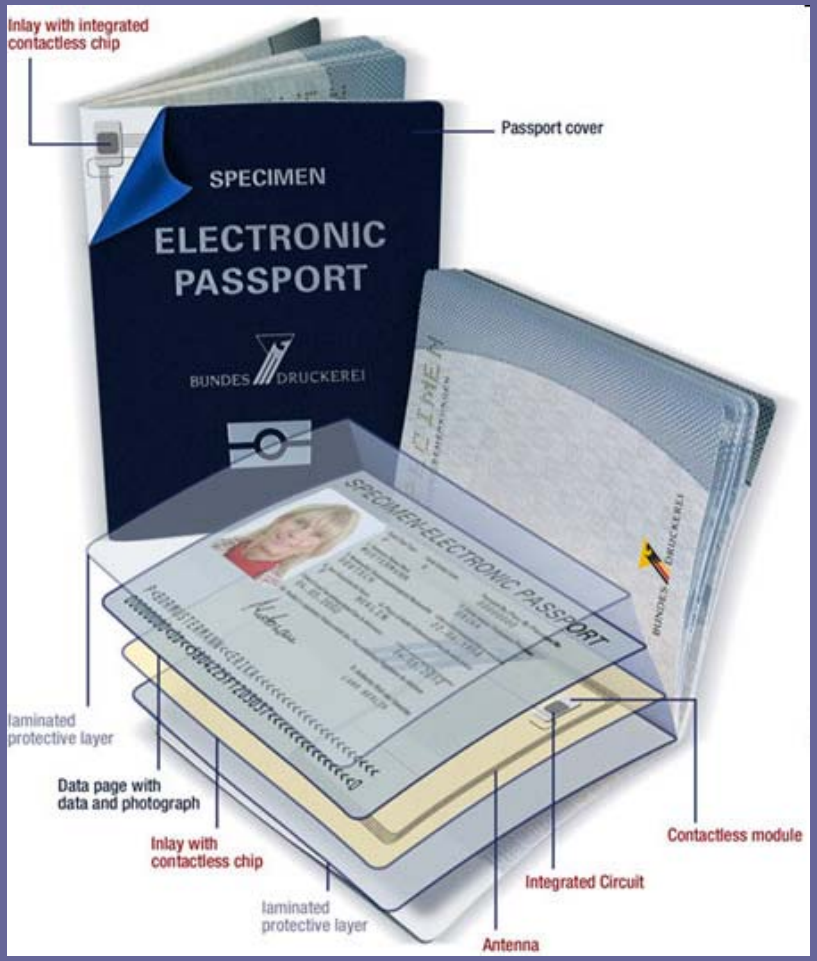
Automated toll-payment transponders

Payment tokens

RFID systems in libraries



Passports



- Already implemented in many different countries
- Biometric data saved on a RFID tag

→More difficult to counterfeit

→Easier to identify people

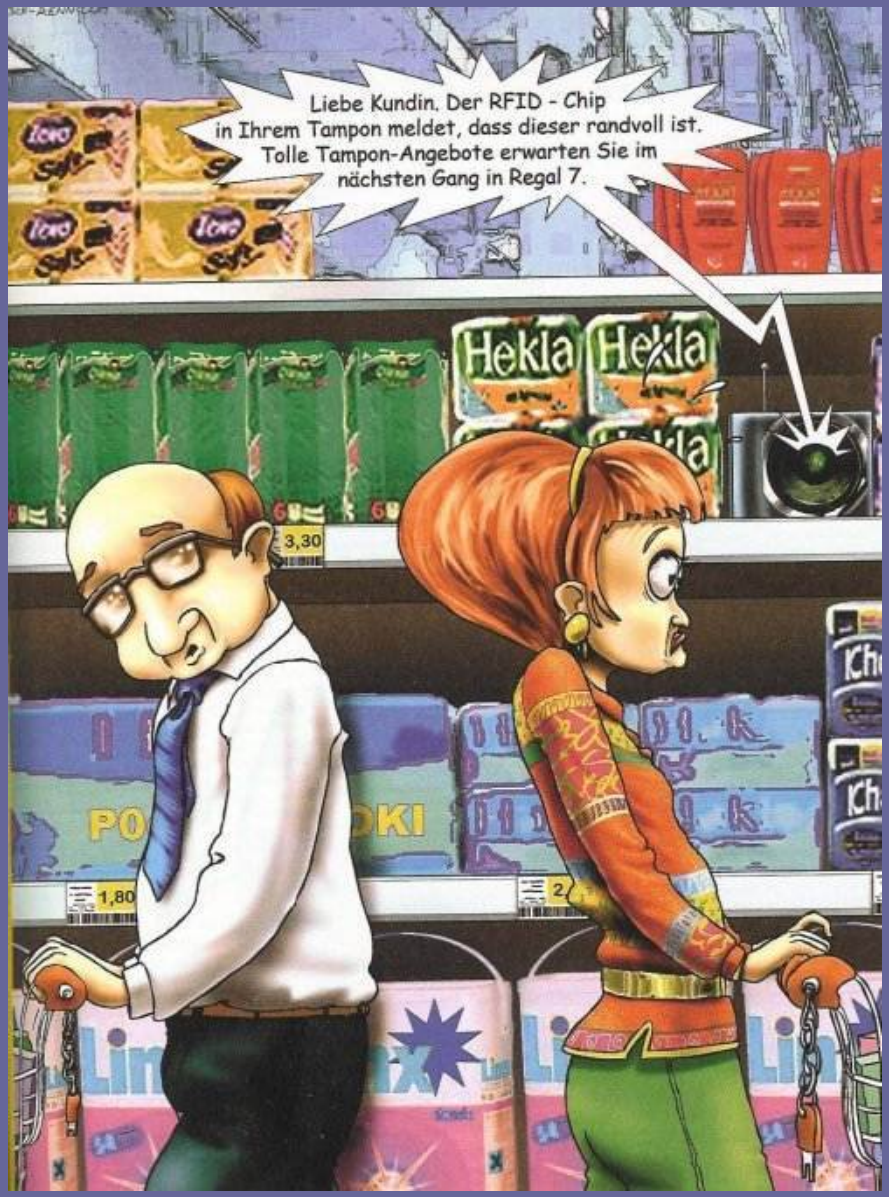
VeriChip – for house pets and humans

- RFID implants already in about fifty million house pets
- Mexico: department of public prosecution implants chips into employees to secure access to a centralized data center for fight against crime

RFID Tomorrow

- Shopping: point-of-sale terminals
- Smart appliances
- Interactive objects
- Medication compliance

Security and Privacy problems



Privacy

- Two main concerns:
  - Clandestine tracking
  - Inventorying

  Problems:

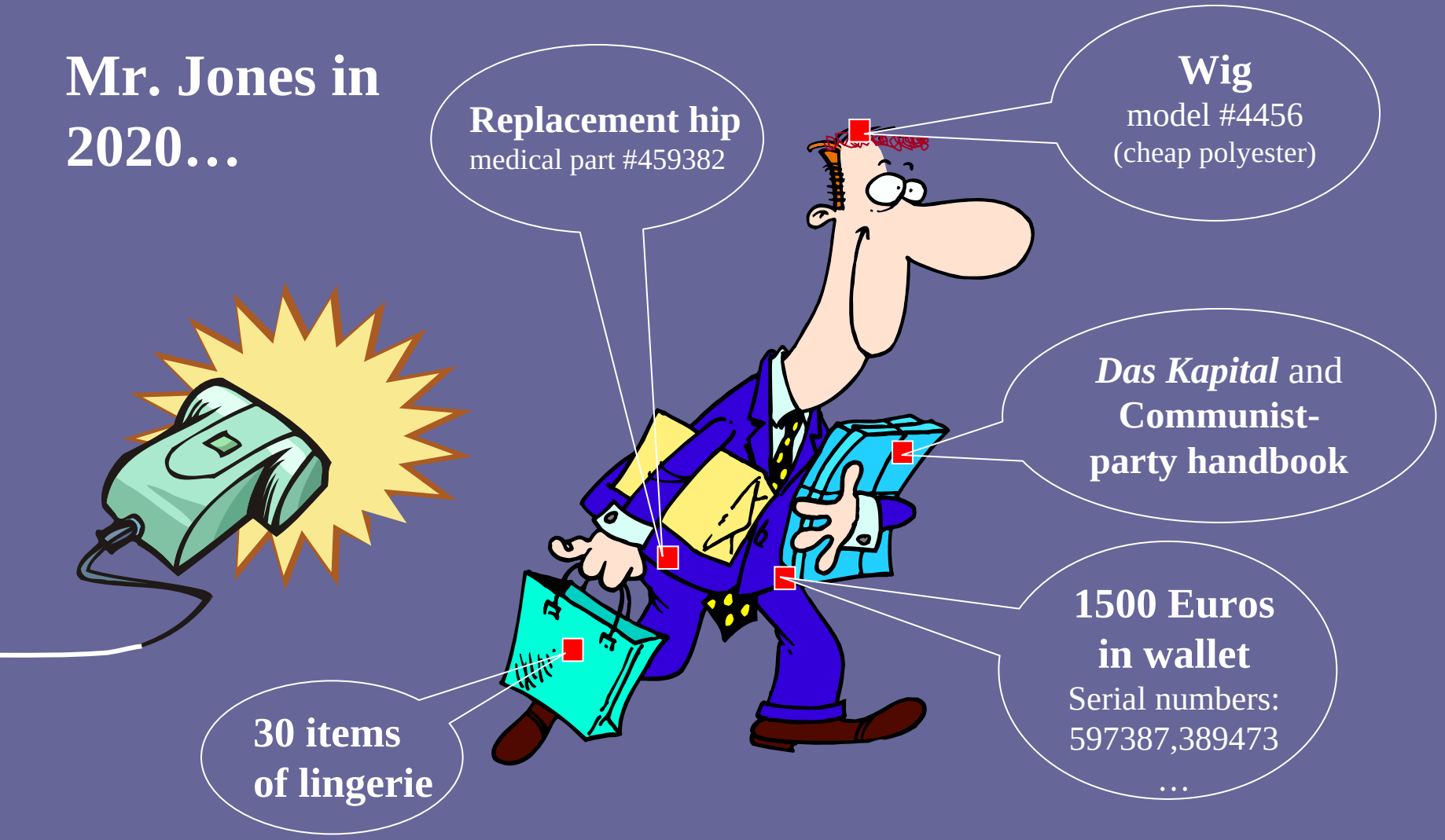
  No alerting of the tag-owners when RFID tags respond to reader

  Threat to privacy grows when tag serial number combined with personal information

  Person carrying EPC tags subject to clandestine tracking

The consumer privacy problem

Mr. Jones in 2020…



Privacy not just a consumer concern

- Eavesdropping: (tag to reader, reader to tag)
  - Enemy forces monitoring RFID communications in a military supply chain
  - Retail market: competitors could learn about stock turnover rates (corporate espionage)
    - U.S. State Department considers encryption of passports

Authentication

- Belief in tag authenticity, but tag counterfeiting (very easy to copy EPC tags → no real guarantee of authenticity)
- RFID tags can help identify sources of counterfeit goods
- Tags for preventing theft in retail shops
- Authentication of distance

Attack models

- Adversaries usually no around-the-clock access
- Physical proximity necessary to scan tag
- “minimalist” security model (Juels)
- “detection” model (Juels, Weis), “prevention” model

Some privacy approaches

BASIC RFID TAGS

Security of basic RFID tags

- No standard cryptographic functions
- Cheap tags that can do no cryptography preferred to expensive tag with cryptography (e.g. by retailers)
- privacy-protecting schemes focused on the consumer privacy problem

Approach 1

- Protect RFID devices by covering them with foil or protective mesh

Approach 2: “Killing” and “Sleeping”

- Problem killing: with killing all useful functions of tag gone
- Problem sleeping: access control for waking of tags confronted by difficulties

The renaming approach

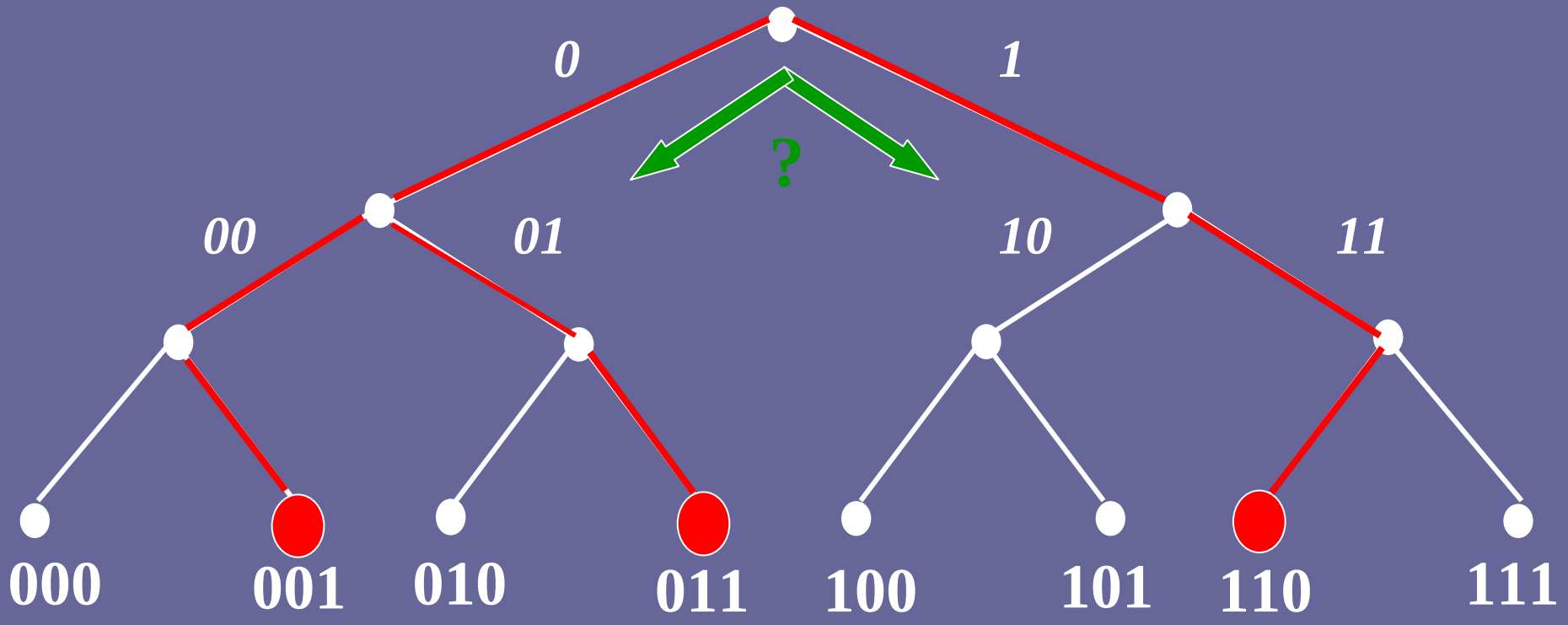
- Encrypting not a solution to prevent tracking
  - Relabeling
  - “Minimalist” Cryptography: pseudonym rotation
  - Re-encryption: public key PK and private key SK
  - Universal re-encryption

Approach 4: Blocking

- Tags contain a modifiable "privacy bit"
- "0" privacy bit: unrestricted public scanning, "1": private
- Within the privacy zone: tag protected by the blocker
- One type of singulation (anti-collision) protocol is "tree-walking"

“Tree-walking”

Blocker protects RFID tag from scanning by simulating collisions in the singulation tree



Soft blocking

- Soft blocker tag always “polite”
- Polite blocking: Blocker informs reader of its presence (e.g. “Do not scan tags whose privacy bit is on”)
- Construction of an audit device
- Advantages:
  - Soft blocker tag is ordinary RFID tag
  - “opt-in” instead of “opt-out” policies

Some privacy approaches

SYMMETRIC - KEY TAGS

Symmetric-key tags

- More security capabilities than Basic tags
- cryptographic one-way functions which rely on a secret key *k*
- Message or plaintext *M* can be encrypted as a ciphertext *C* with key *k*
- *k* is necessary to decrypt *C* and recover *M*

Cloning

- simple challenge – response protocol: Tag *T* can authenticate itself to a reader (both share the key *k*)
- → when hash function h well constructed and appropriately deployed, no attacker can simulate T successfully without physically attacking the tag
- Digital Signature Transponder (DST): e.g. chip in the ignition key, team of researchers fully cloned DST tokens
- Side-channel attacks: timing attacks, power analysis attacks
- Relay or man-in-the-middle-attacks: these attacks can bypass any cryptographic protocol; countermeasures e.g. tag localisation

Approaches avoiding brute-force key search

- Tree approach
- Synchronization approach
- Time-space tradeoff approach

DISCUSSION

RFID Chips – Eine geniale Erfindung oder George Orwell laesst gruessen?