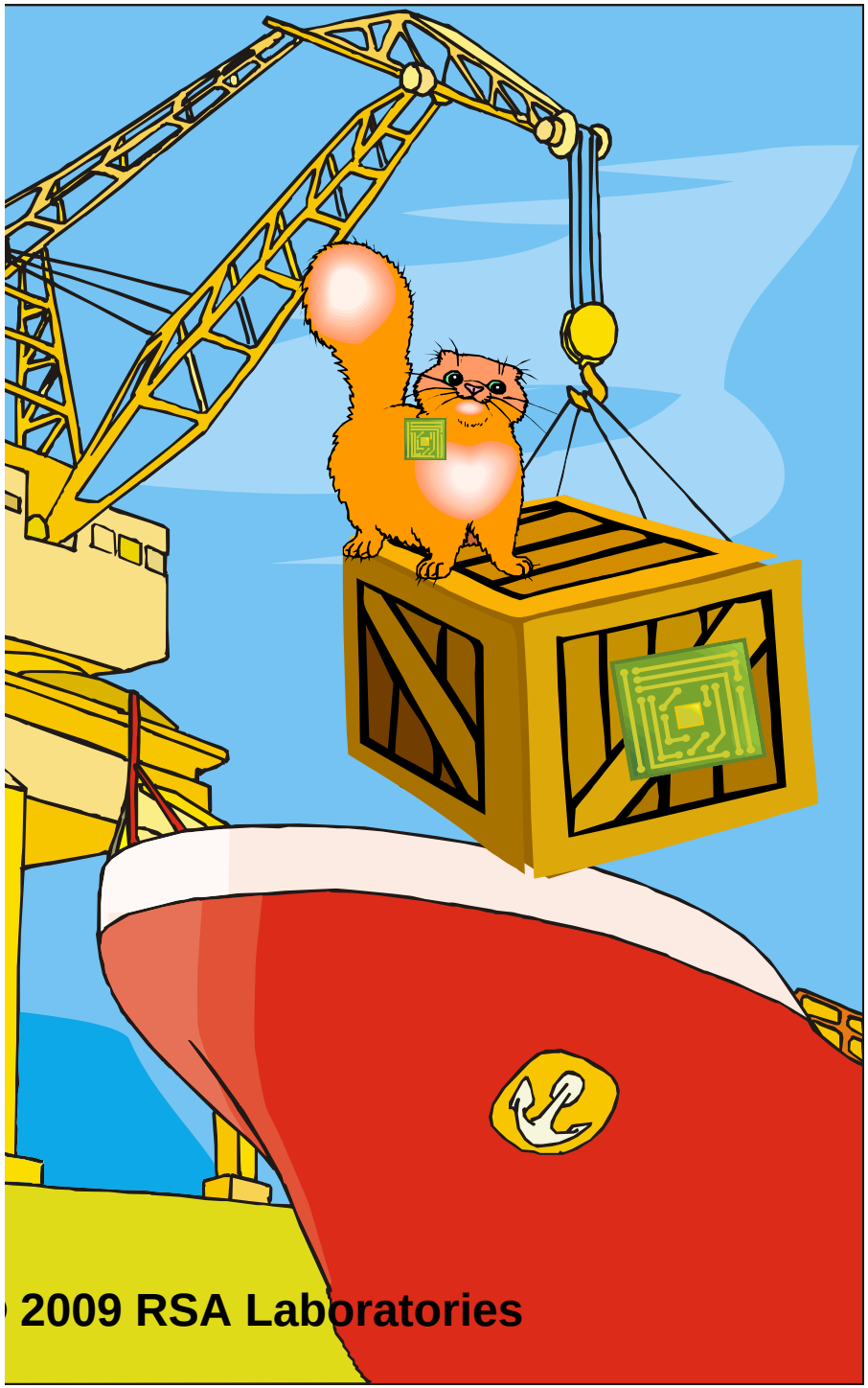


RFID Security and Privacy: A Primer

Ari Juels
RSA Laboratories

ENISA-FORTH NIS
15 September 2009

RFID (Radio-Frequency IDentication) takes many forms…



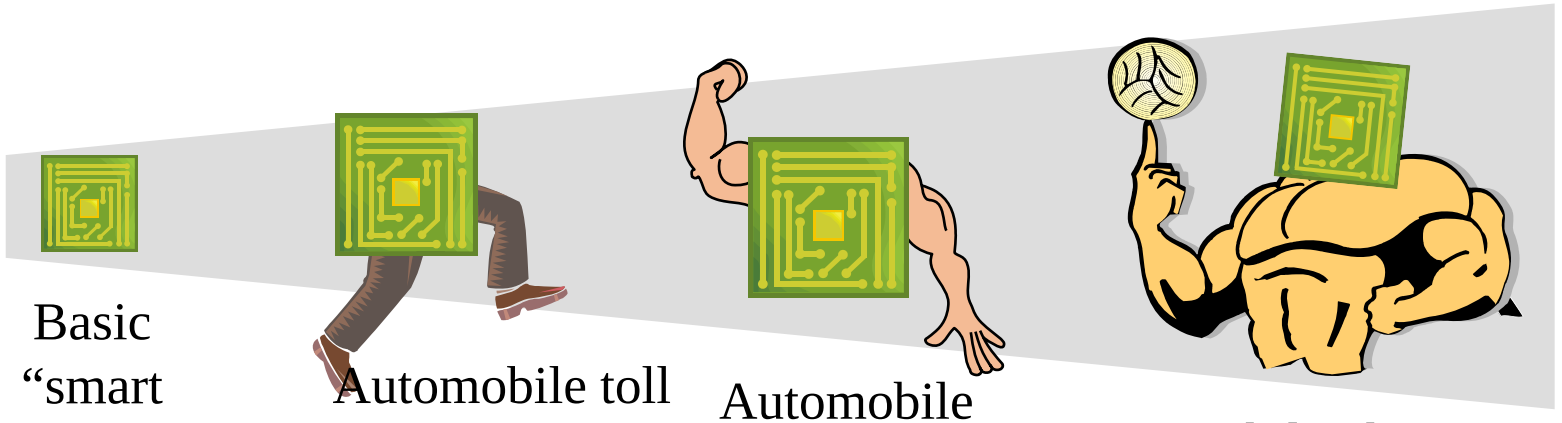








“RFID” really denotes a spectrum of devices



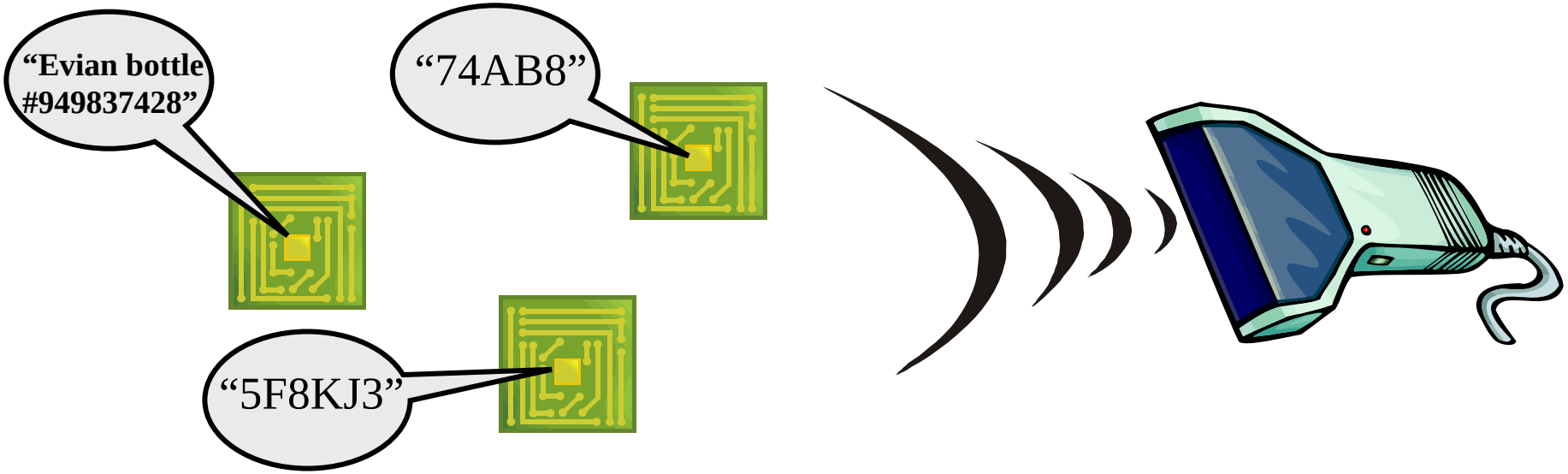
Basic “smart label”	Automobile toll payment plaque	Automobile ignition key	Mobile phone
no battery	*battery*	*no battery*	
no crypto	*no crypto*	*some crypto*	
few cm to few meters range	*several meters range*	*several cm range*	

Some nomenclature

- Passive tag: Receives power from reader
- Active tag: Battery to initiate communication
- Semi-passive tag: Battery for return response
- Contactless smartcard: Short-range wireless device, usually passive and with some crypto
- Sensor: Wireless device that transmits environmental data
- **RFID**: Any wireless device whose main function is identification of an object…

“Smart label” RFID tag

- Passive tag
- Range of up to several meters
- Simply calls out (unique) name and static data



Capabilities of “smart label” RFID tag

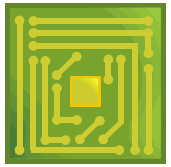
- Little memory
  - Static 96-bit+ identifier in current ultra-cheap tags
  - Hundreds of bits soon
- Little computational power
  - Several thousand gates (mostly for basic functionality)
  - ***No* real cryptographic functions possible**

“Smart labels”: EPC (Electronic Product Code) tags

Barcode



EPC tag



Line-of-sight

Radio contact

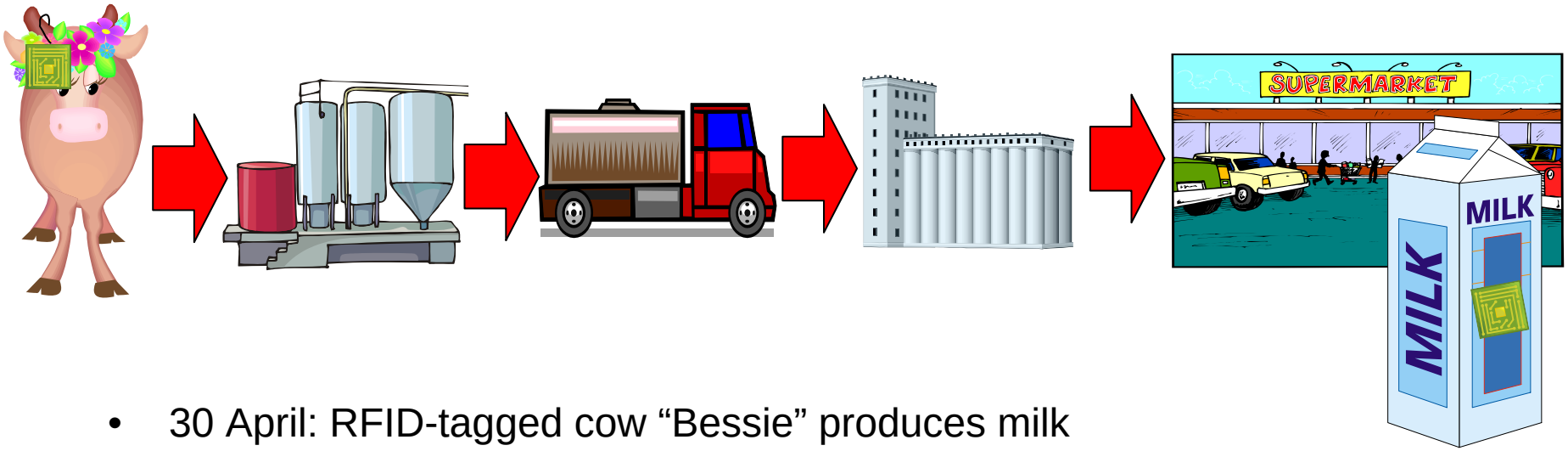
Fast, automated scanning

Specifies object type

Uniquely specifies object

Provides pointer to database entry for every object, i.e., unique, detailed history

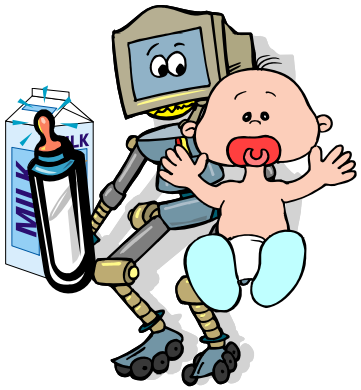
2030: Week in the life of a milk carton

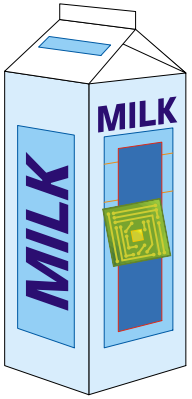


- 30 April: RFID-tagged cow “Bessie” produces milk
- 30 April: Milk transferred to RFID-tagged tank
  - Cow identity and milking time recorded in tank-tag database
- 1 May: RFID portal on truck records loading of refrigeration tanks
  - (Truck also has active RFID (+GPS) to track geographical location and RFID transponder to pay tolls)
- 2 May: Chemical-treatment record written to database record for milk barrel
  - Bessie’s herd recorded to have consumed bitter grass; compensatory sugars added
- 3 May: Milk packaged in RFID-tagged carton; milk pedigree recorded in database associated with carton tag
- 4 May: RFID portal at supermarket loading dock records arrival of carton
- 5 May: “Smart” shelf records arrival of carton in customer area
- 5 May 0930h: “Smart” shelf records removal of milk
- 5 May 0953h: Point-of-sale terminal records sale of milk (to Alice)

2030: Week in the life of a milk carton

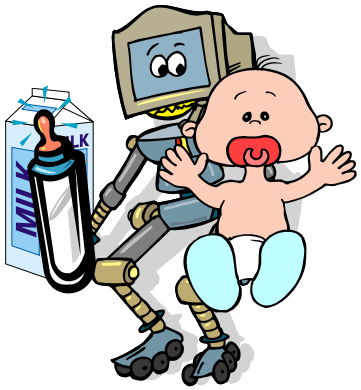
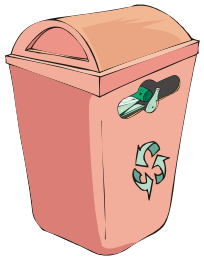


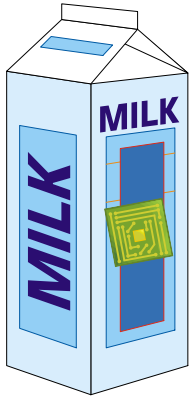




- 6 May 0953h: Supermarket transfers tag ownership to Alice's smart home
- 6 May 1103h: Alice's refrigerator records arrival of milk
- 6 May 1405h: Alice's refrigerator records removal of milk; refrigerator looks up database-recorded pedigree and displays: "*Woodstock, Vermont, Grade A, light pasturization, artisanal, USDA organic, breed: Jersey, genetic design #81726*"
- 6 May 1807h: Alice's "smart" home warns domestic robot that milk has been left out of refrigerator for more than four hours
- 6 May 1809h: Alice's refrigerator records replacement of milk
- 7 May 0530h: Domestic robot uses RFID tag to locate milk in refrigerator; refills baby bottle

2030: Week in the life of a milk carton

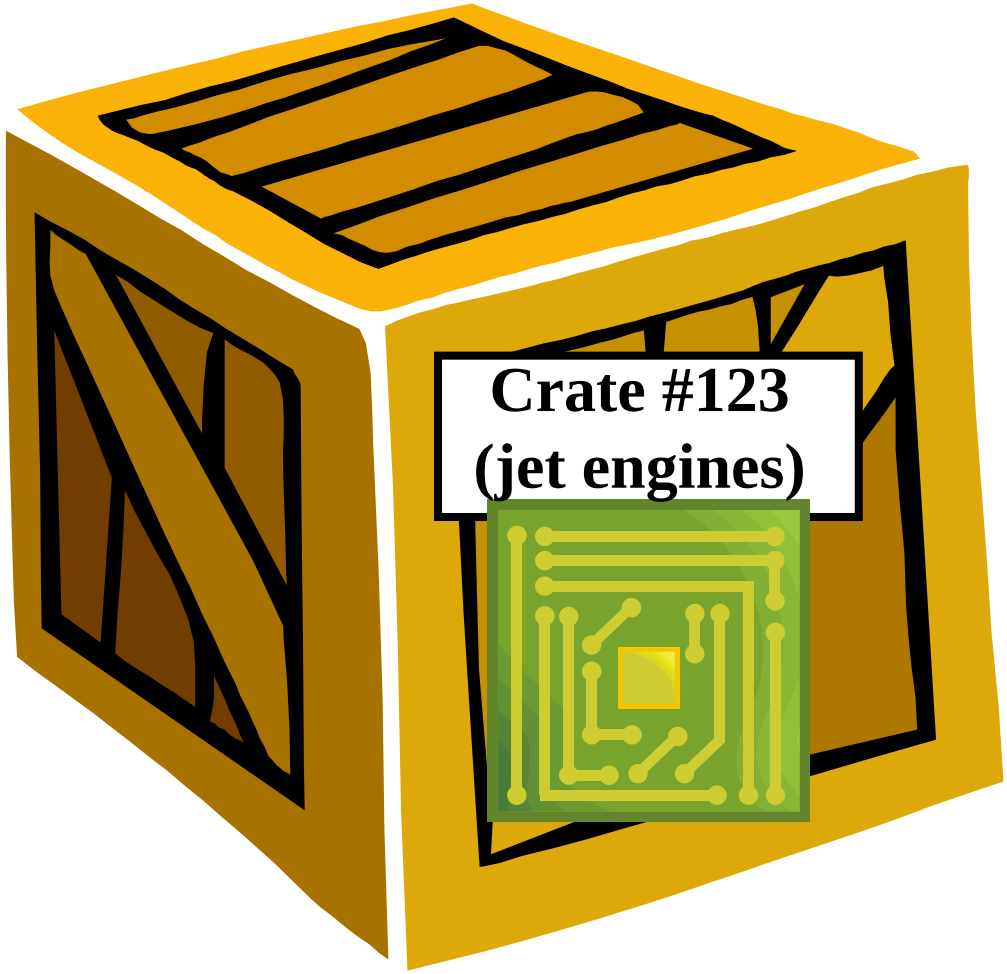






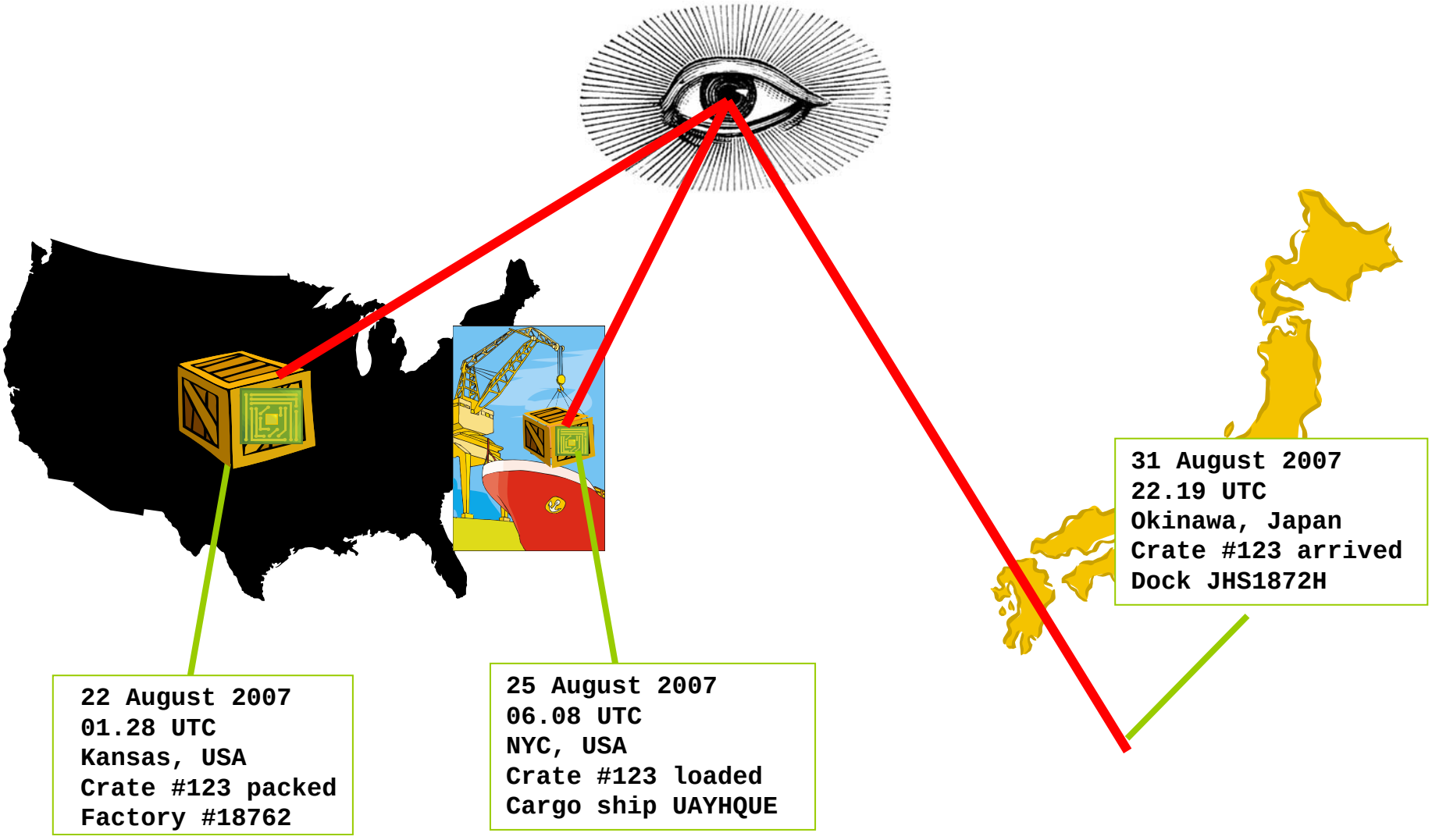
- 6 May 0953h: Supermarket transfers tag ownership to Alice's smart home
- 6 May 1103h: Alice's refrigerator records arrival of milk
- 6 May 1405h: Alice's refrigerator records removal of milk; refrigerator looks up database-recorded pedigree and displays: "*Woodstock, Vermont, Grade A, light pasturization, artisanal, USDA organic, breed: Jersey, genetic design #81726*"
- 6 May 1807h: Alice's "smart" home warns domestic robot that milk has been left out of refrigerator for more than four hours
- 6 May 1809h: Alice's refrigerator records replacement of milk
- 7 May 0530h: Domestic robot uses RFID tag to locate milk in refrigerator; refills baby bottle
- 7 May 0531h: Robot discards carton; "Smart" refrigerator notes absence of milk; transfers order to Alice's PDA/phone/portable server grocery list
- 7 May 2357h: Recycling center scans RFID tag on carton; directs carton to paper-brick recycling substation

RFID Today

Not item-level, but cases and pallets



Supply-chain visibility



RFID TODAY: IN YOUR POCKET

Note: Often just emit static identifiers, i.e., they are just smart labels!





Proximity cards

IN YOUR POCKET

RFID helps secure hundreds of millions of automobiles

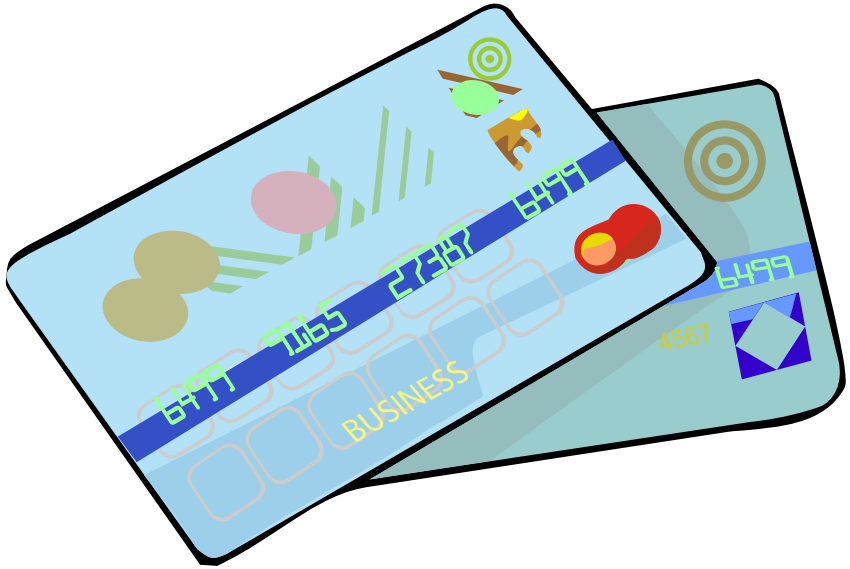
- Cryptographic challenge-response
- Philips claims more than 90% reduction in car theft thanks to RFID!
- Note: some devices, e.g., Texas Instruments DST, are weak (Bono et al.)…



Automobile ignition keys

IN YOUR POCKET

- RFID now offered in all major credit cards in U.S.…
- Many are cryptographically enabled
- “Vulnerabilities in First-Generation RFID-Enabled Credit Cards”
  - T. Heydt-Benjamin, D. Bailey, K. Fu, A. Juels, and T. O’Hare



Payment devices

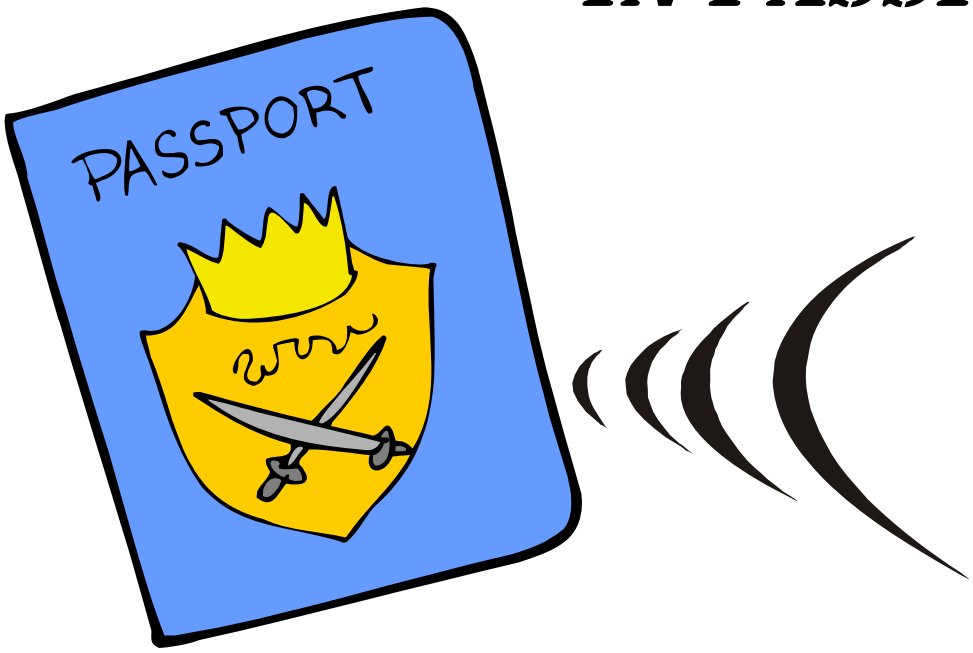
IN MOBILE PHONES

NFC (Near-Field Consortium)



- Also, ticket purchases, payments, comparison shopping
  Phone can act as reader or tag
- NFC is a general-purpose protocol
- Already available in some models

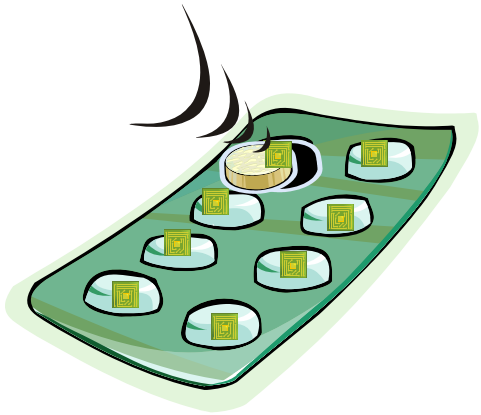
IN PASSPORTS

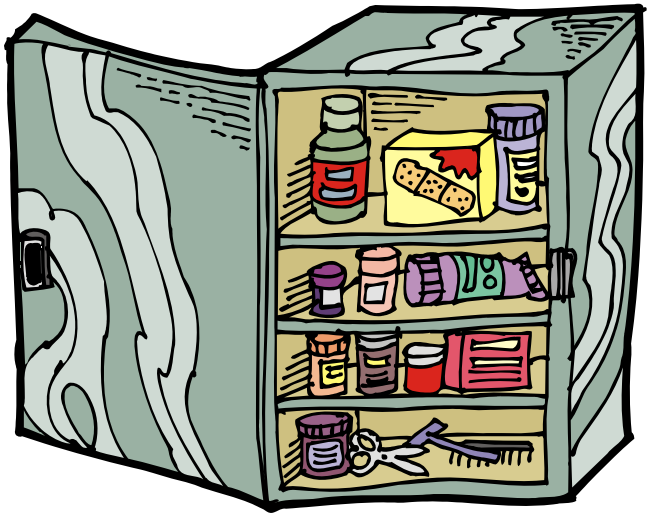


- Dozens of countries issuing RFID-enabled passports
- Other identity documents, e.g., drivers' licenses as well

IN PHARMACEUTICALS

- Anti-counterfeiting: Better supply-chain visibility means less fraud
  - U.S. govt. urging RFID to combat counterfeiting of drugs
- Medical compliance: Greater independence (and privacy!), particularly for elderly





IN CURRENCY?



- Talk in 2003-4 of planting RFID tags in 10,000 Yen banknotes and Euro banknotes
- Talk has dissipated
- Main interest: anti-counterfeiting

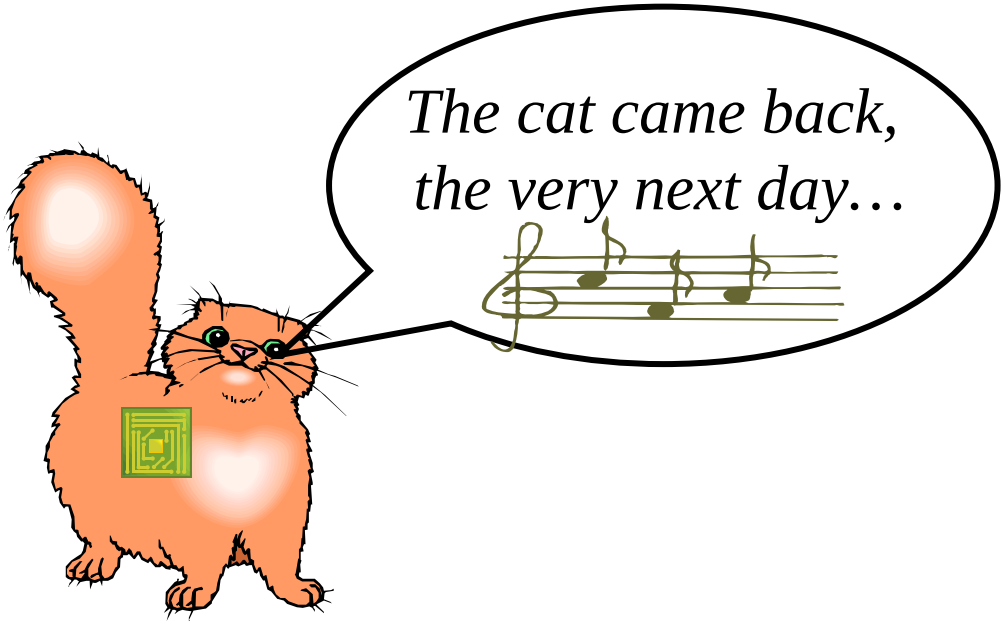
IN ANIMALS

- Livestock

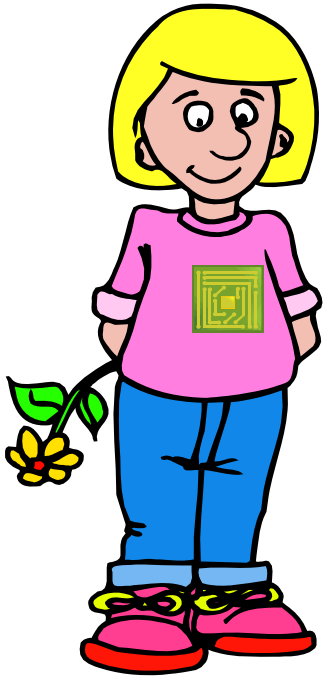


- Housepets

50 million+



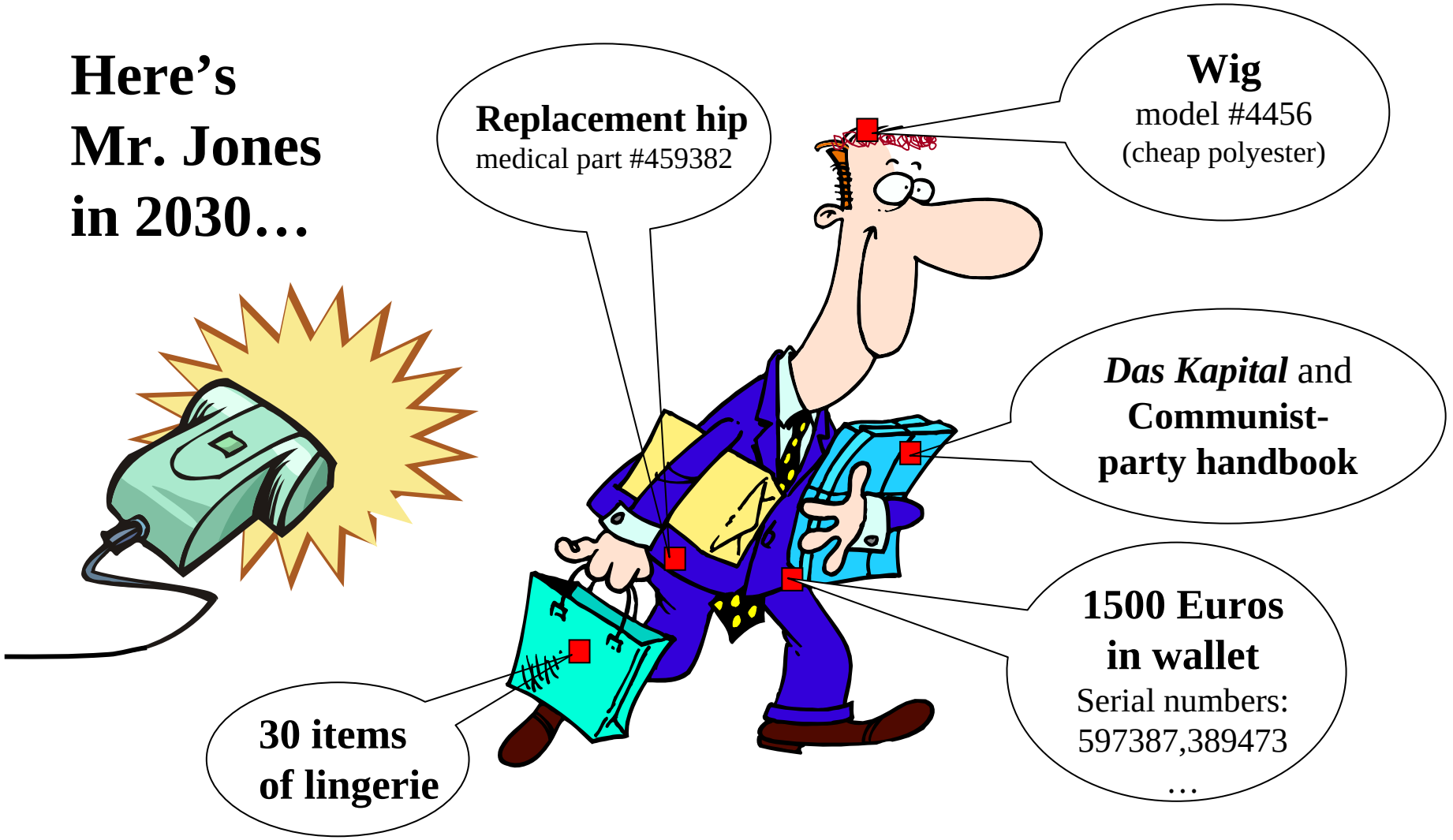
ON PEOPLE



- Schools
- Amusement parks
- Hospitals
- In the same vein: mobile phones with GPS…

Security and Privacy Challenges

The consumer privacy problem



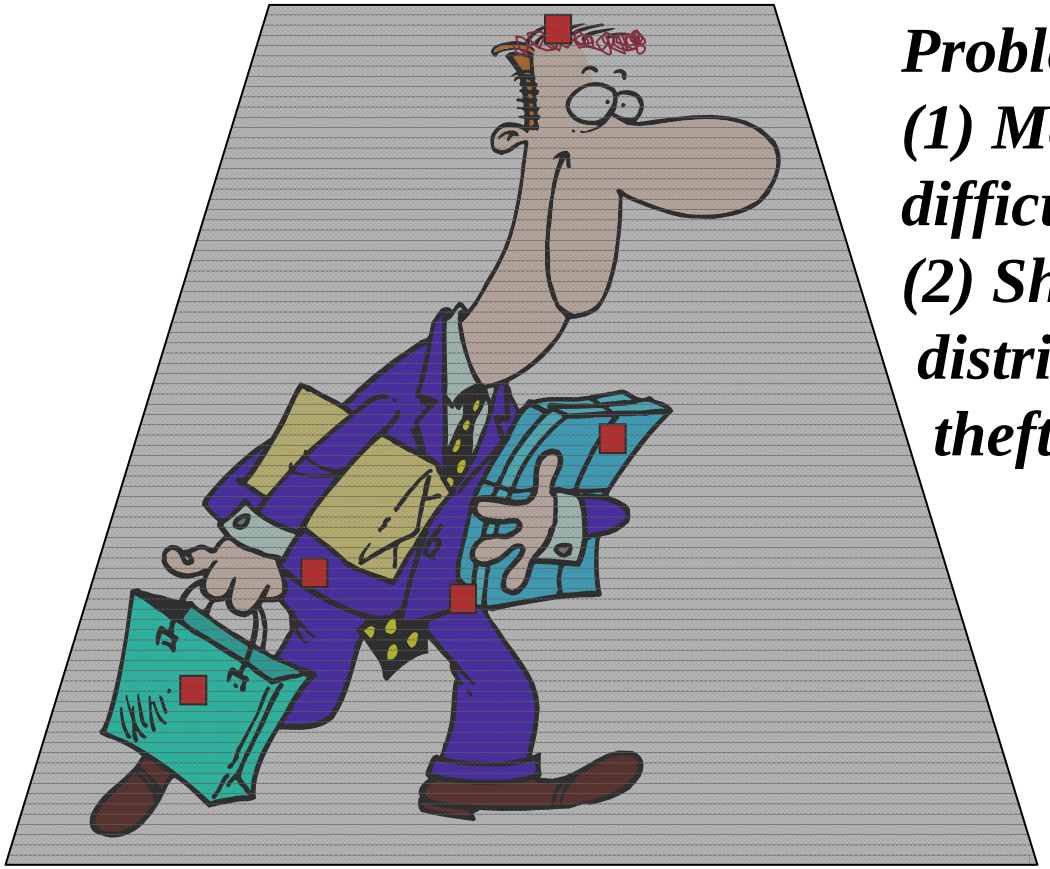
© RSA Laboratories

…and the tracking problem



- Mr. Jones attends a political rally; law enforcement scans his RFID tags
- Mr. Jones wins Turing Award; physically tracked by paparazzi via RFID

Approach 1: Cover RFID tags with protective mesh or foil



Problems:
(1) Makes locomotion difficult
(2) Shops don't like distributing tools for theft

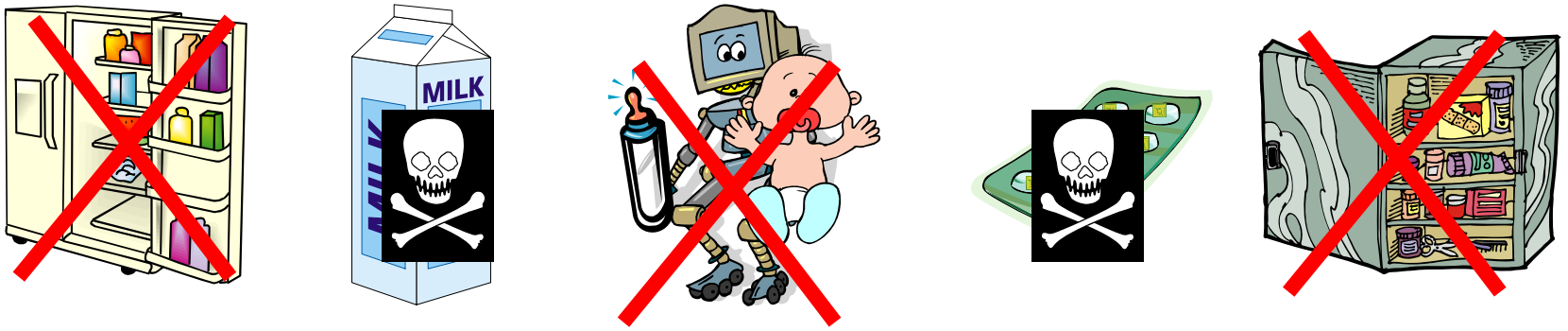
Approach 2:
EPC “kill” command for RFID tags



Problem:
RFID tags are much too useful in “live” state…

We are already carrying RFID tags, and then…

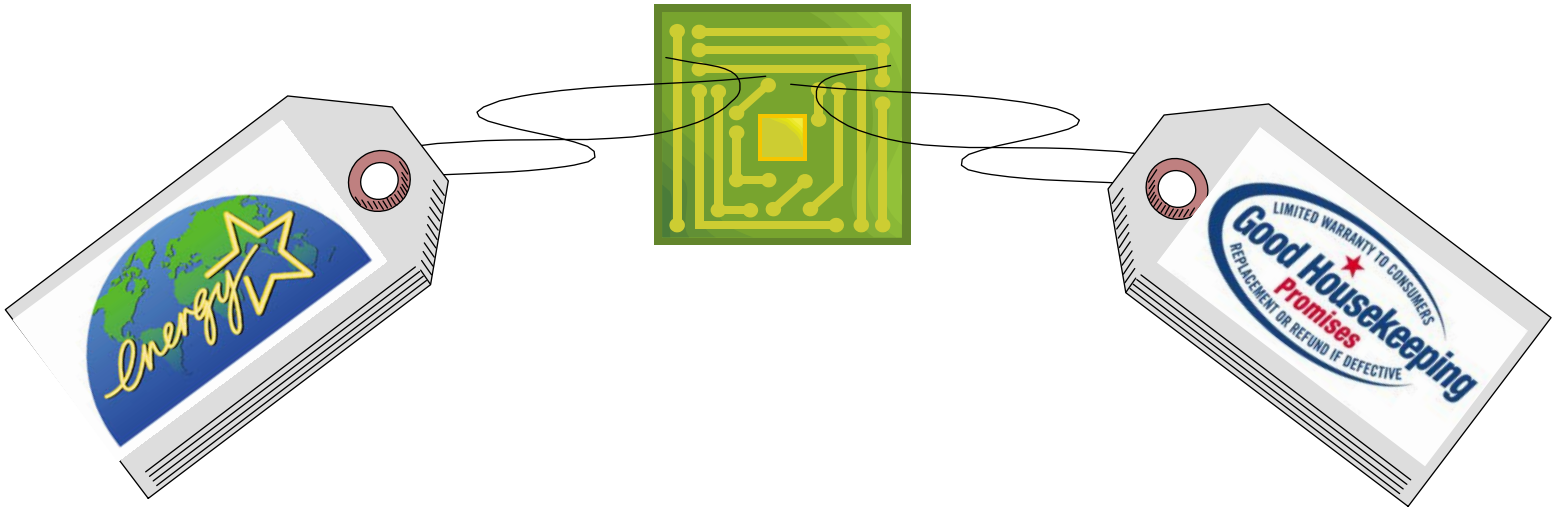
Post-consumer uses of tags



Dead tags perhaps not harmful, but certainly not beneficial…

Approach 3: Policy and legislation

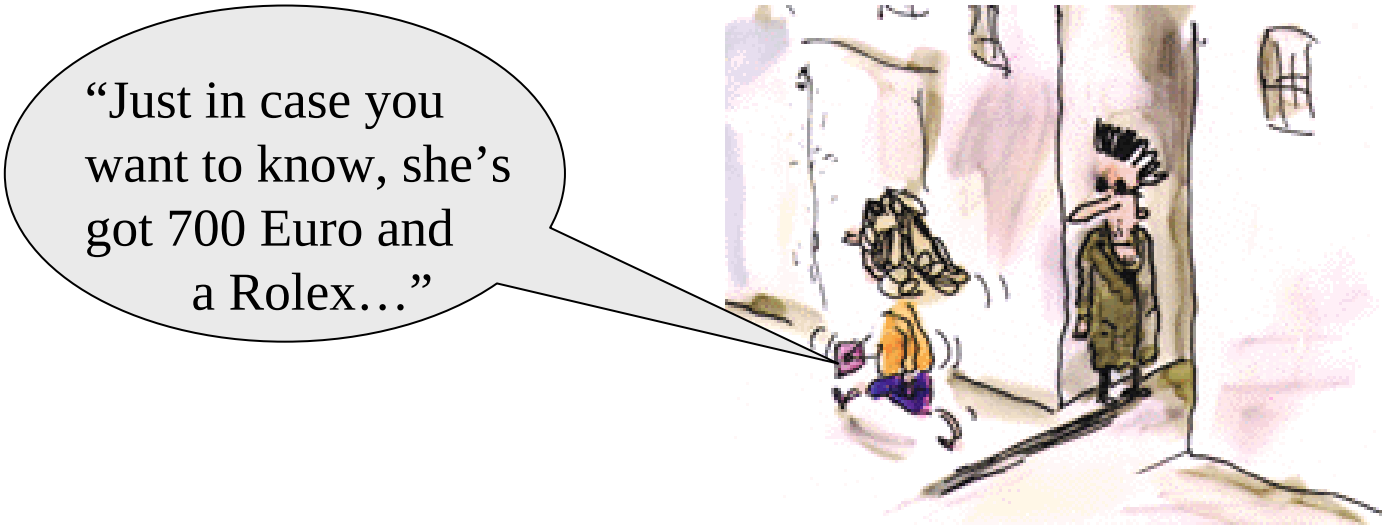
- Undoubtedly helpful if carefully thought out, but…
- “Good Housekeeping” seal



- Retailer’s guarantee means little since tags may be read by anyone!
- EU Data Privacy Directive

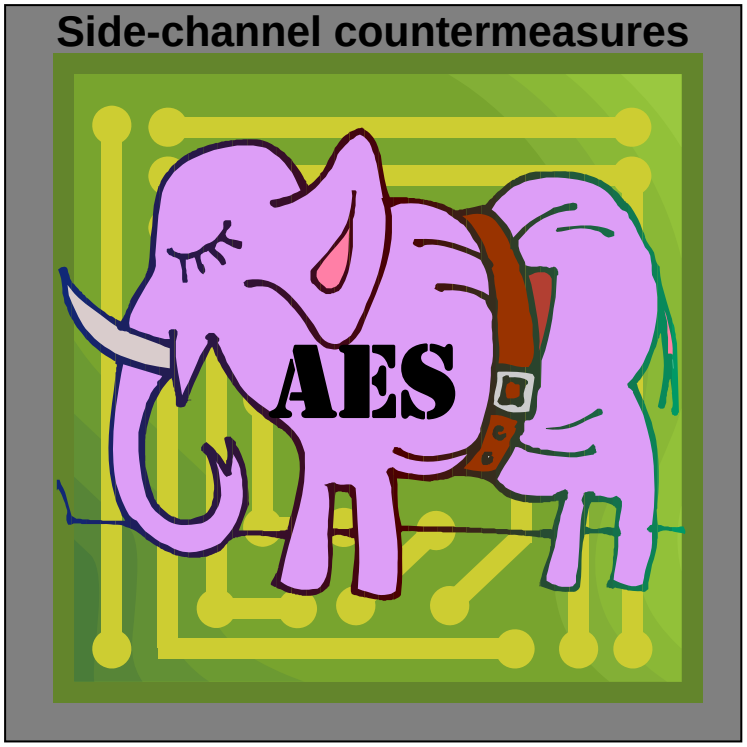
Another possible use of RFID

More efficient mugging



Whom will the EU prosecute now?

Approach 4: Use cryptography



With crypto, we can do:

- Challenge-response for authentication
- Mutual authentication and/or encryption for privacy

But:

1. Moore's Law vs. pricing pressure for EPC
2. The theme of today's talk: The really hard part is **key management…**

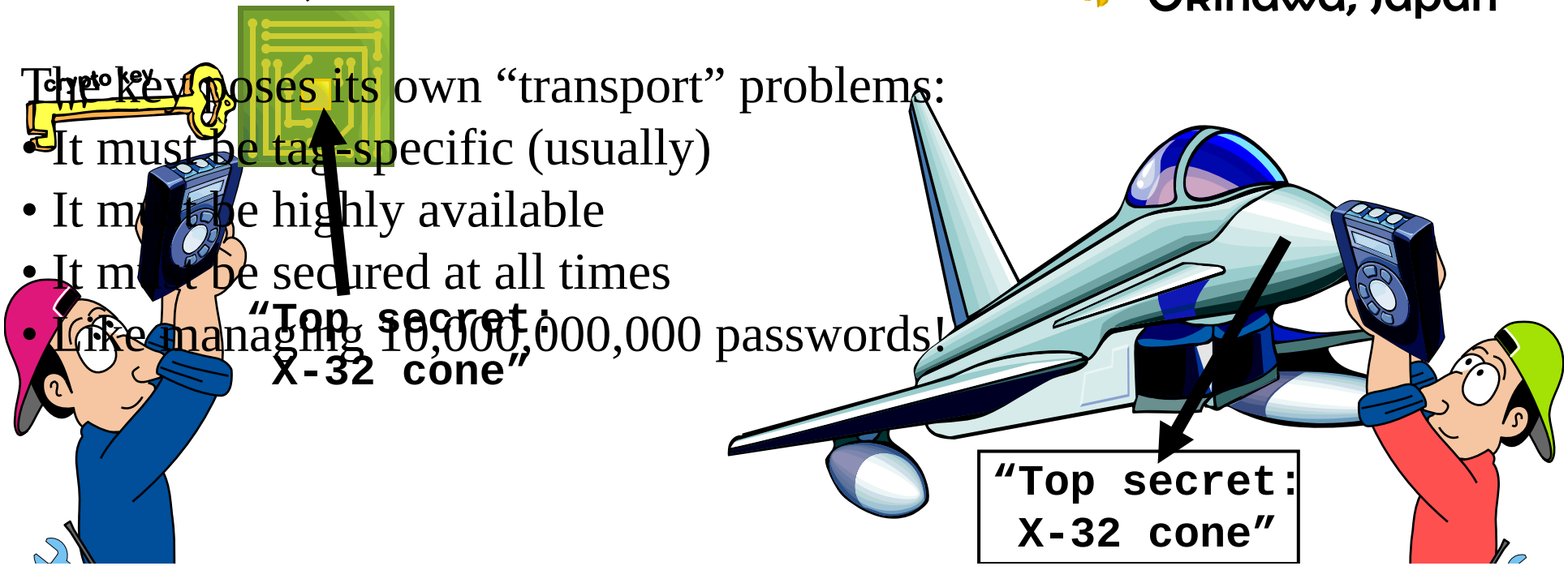
The key-management problem



Kansas, USA



Okinawa, Japan

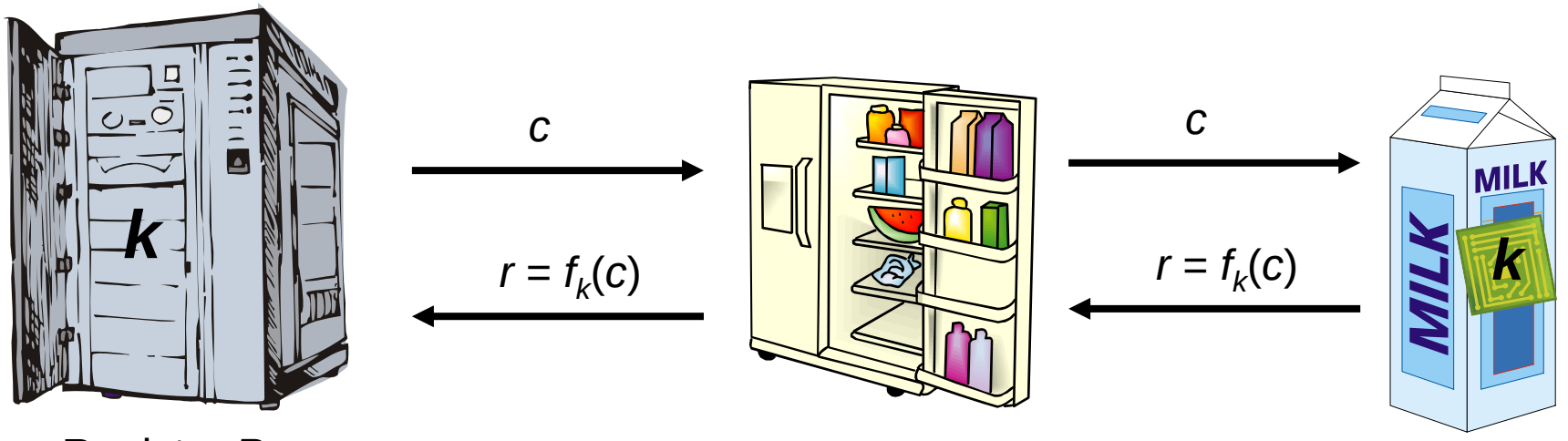


The key poses its own "transport" problems:

- It must be tag-specific (usually)
- It must be highly available
- It must be secured at all times
- Like managing 10,000,000,000 passwords!

Simple authentication: Possession is the law

- How does Alice's refrigerator get read/write privileges for the history for the milk carton bearing tag *T*?
- The straightforward approach:
  - A central registry *R* shares symmetric key *k* with the tag *T*
  - Alice's refrigerator acts as authentication proxy between *R* and *T*
  - Tag *T* authenticates via challenge-response



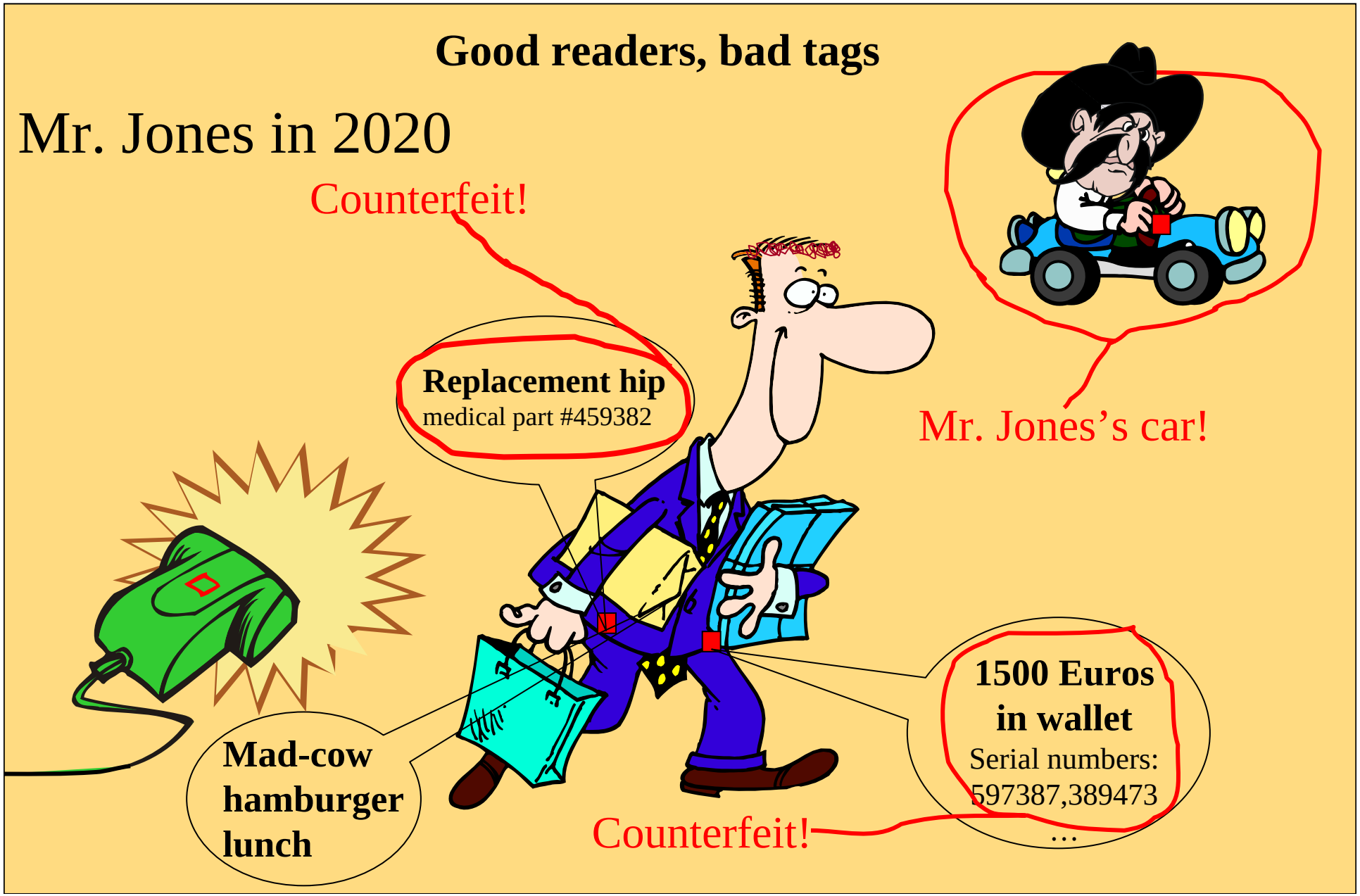
Registry *R*

Simple authentication: Possession is the law

- But what if the tag is on Alice's wristwatch?
  - Should any nearby reader be able to read tag history?
  - Should any nearby reader be able to *modify* tag history?
- What if registry *R* is unavailable?
  - Will the tag carry information on board?
  - If so, who can access it?
  - Does Alice's baby get its milk?



The authentication problem



Two Case Studies

Case 1:
Consumer product privacy

Joint work with

Bryan Parno and Ravi Pappu

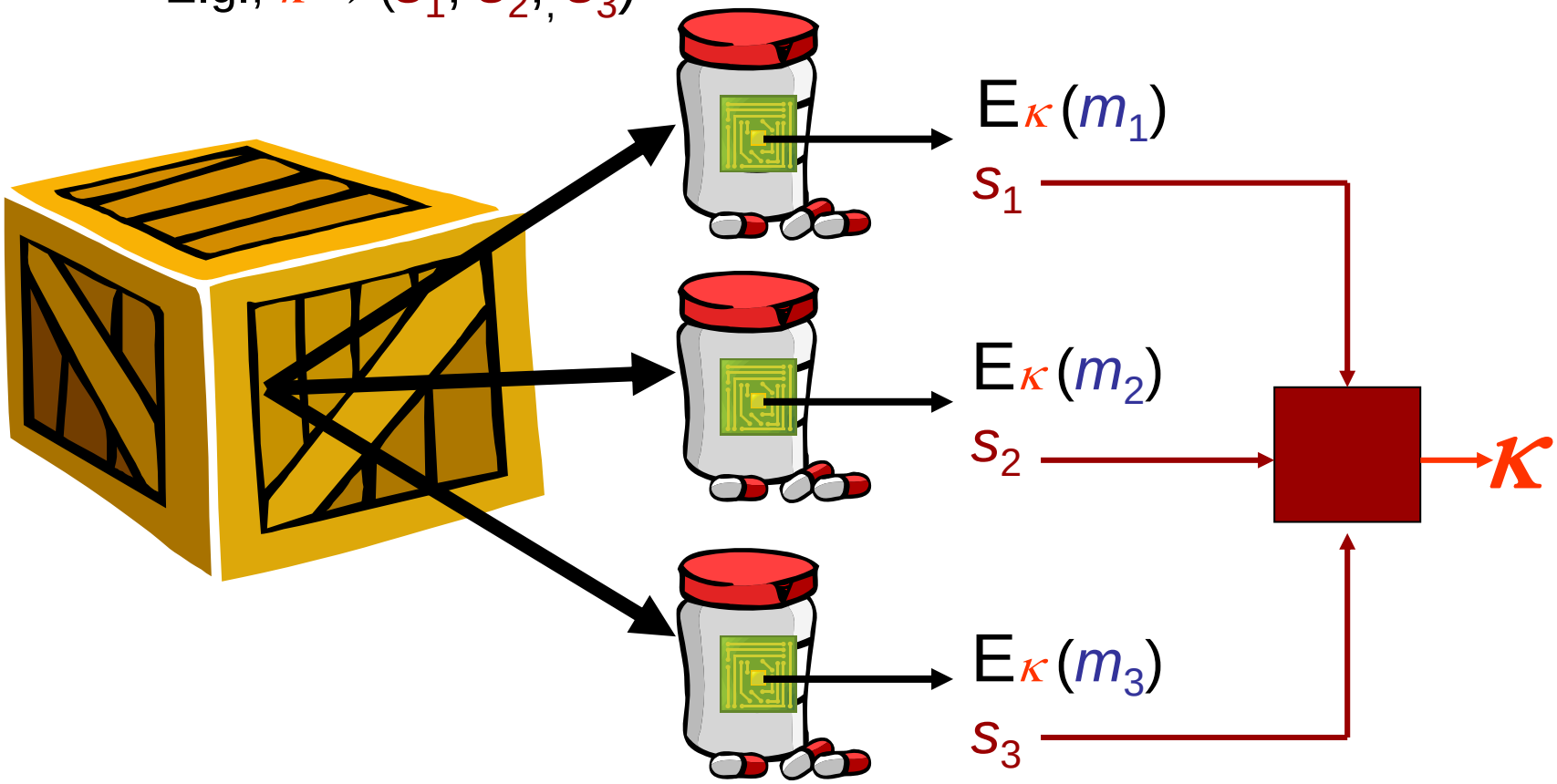
USENIX Security ’08

EPC tags and privacy

- In principle, “kill” is a strong privacy-protecting feature
  - Dead tags tell no tales—solves the Mr. Jones problem
- But commercial RFID users say they:
  - Don’t want the overhead of killing at point-of-sale
  - Don’t want to manage kill PINs
  - Have no channel to communicate secret keys downstream in supply chain
- ***Key management is a big problem!!!***

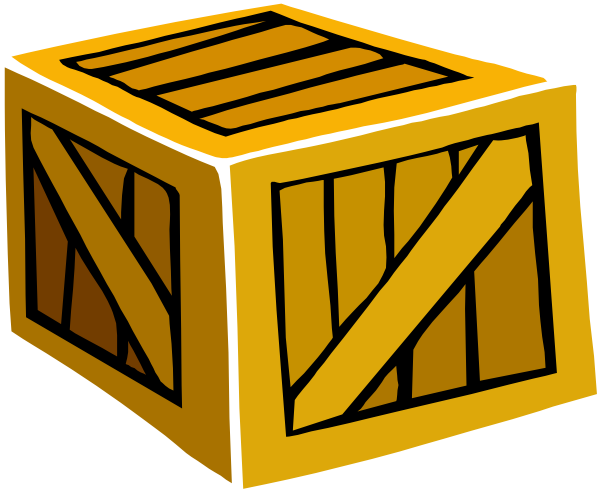
A new, counterintuitive approach: Put secret keys on the tags

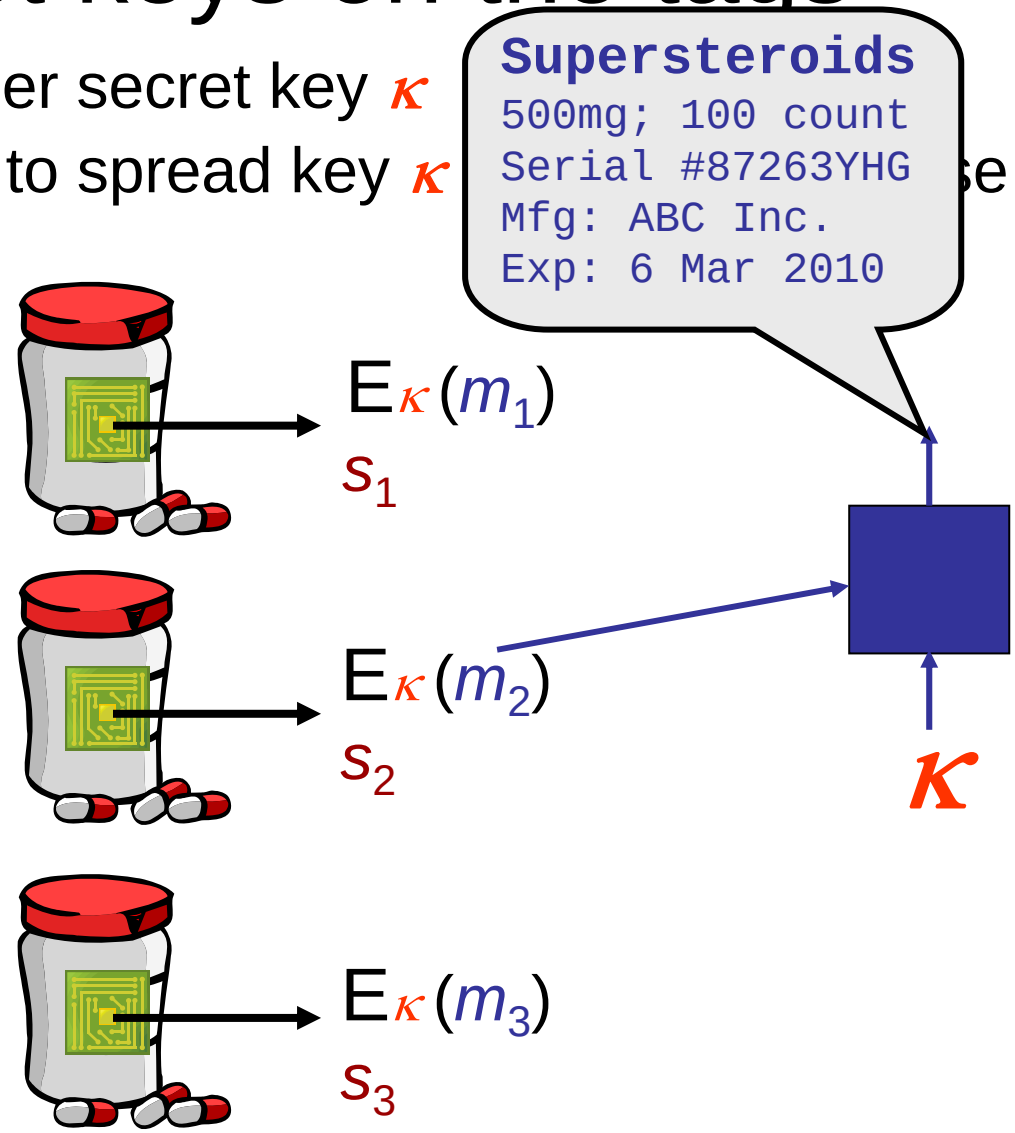
- ***Encrypt*** tag data under secret key κ
- Apply ***secret sharing*** to spread key κ across tags in case
  - E.g., $\kappa \rightarrow (s_1, s_2, , s_3)$



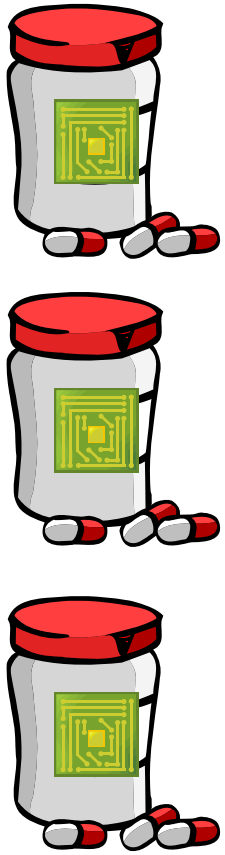
A new approach: Put secret keys on the tags

- ***Encrypt*** tag data under secret key κ
- Apply ***secret sharing*** to spread key κ se
  - E.g., $\kappa \rightarrow (s_1, s_2, s_3)$

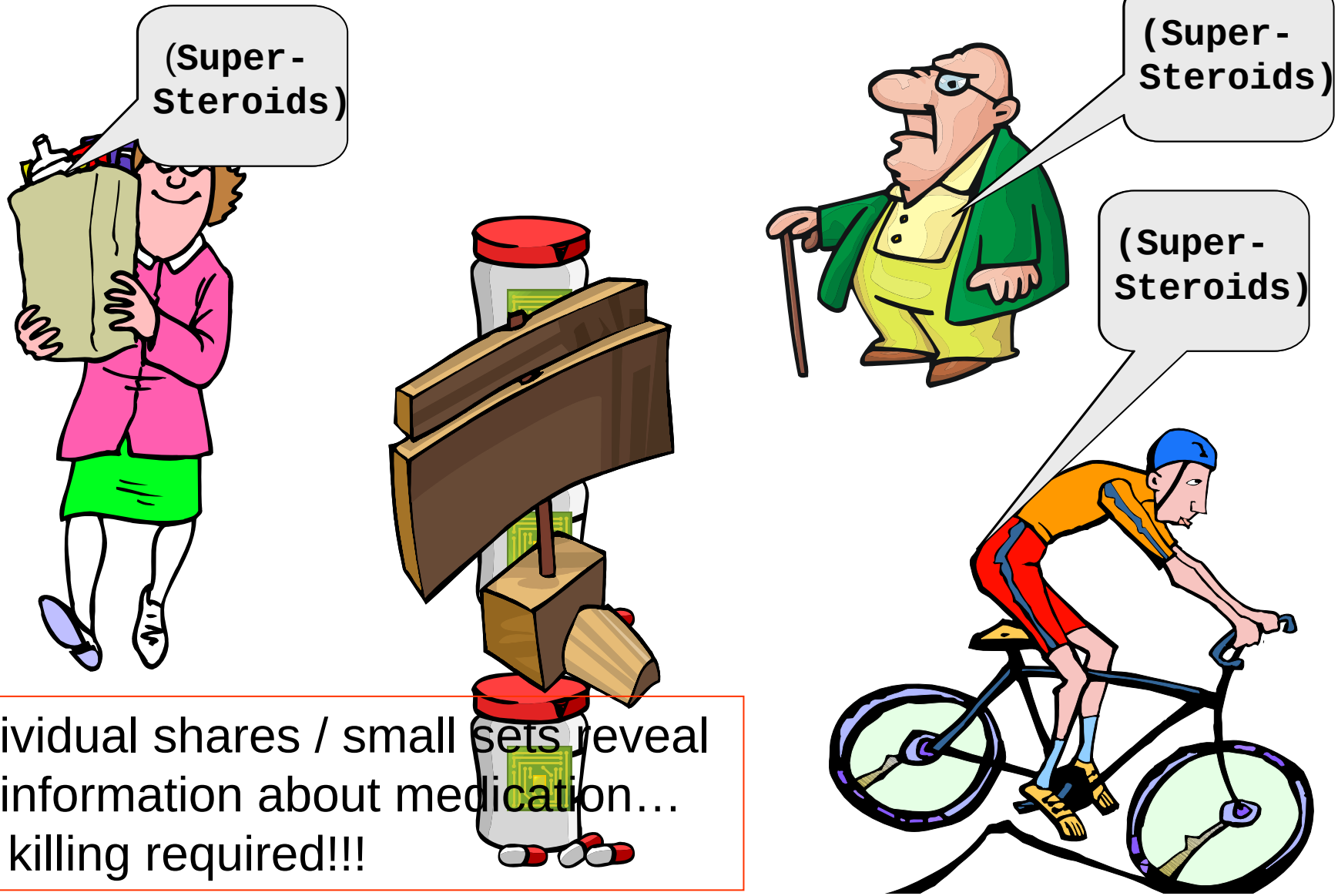




Privacy through dispersion



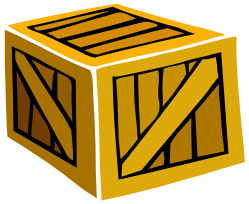
Privacy through dispersion



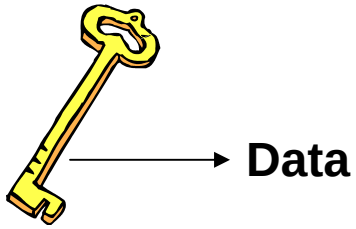
Individual shares / small sets reveal no information about medication…
No killing required!!!

Example application: Privacy protection on medications

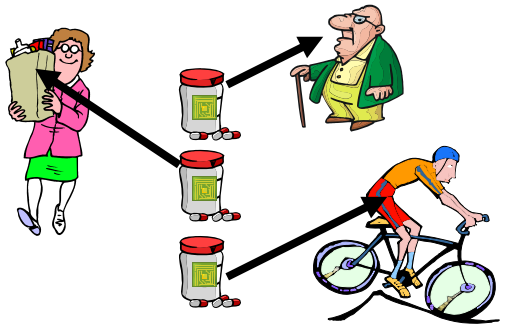




Step 1: Receive case at pharmacy



Step 2: Pharmacy reads tags, gets keys, decrypts data for its database



Step 3: Tags and data are dispersed

Note: We don’t solve the tracking problem!

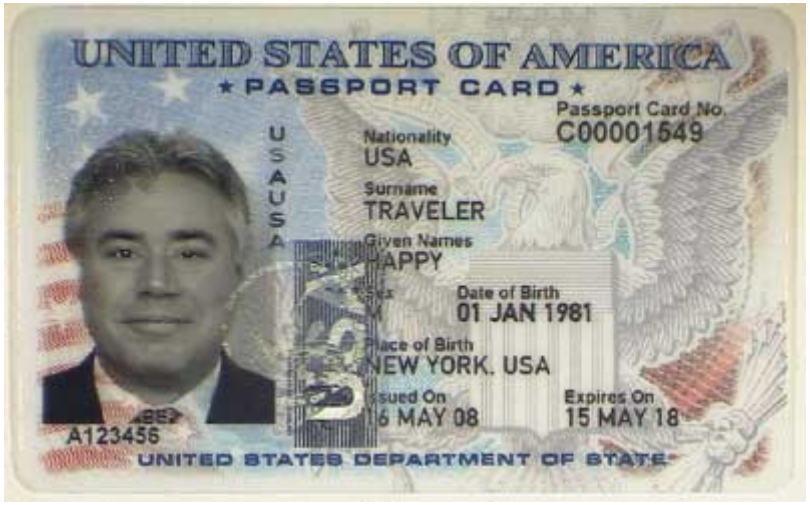


- The share / ciphertext combination is static
- I’d argue that this problem is insoluable / not worth solving…

Case 2: EPC-Tagged Identity Documents

Joint work with
Karl Koscher, Vjekoslav Brajkovic, and Yoshi Kohno
(To appear in ACM CCS ’09)

Passport Cards and Enhanced Drivers Licences (EDLs)





Contains an EPC Gen-2 tag

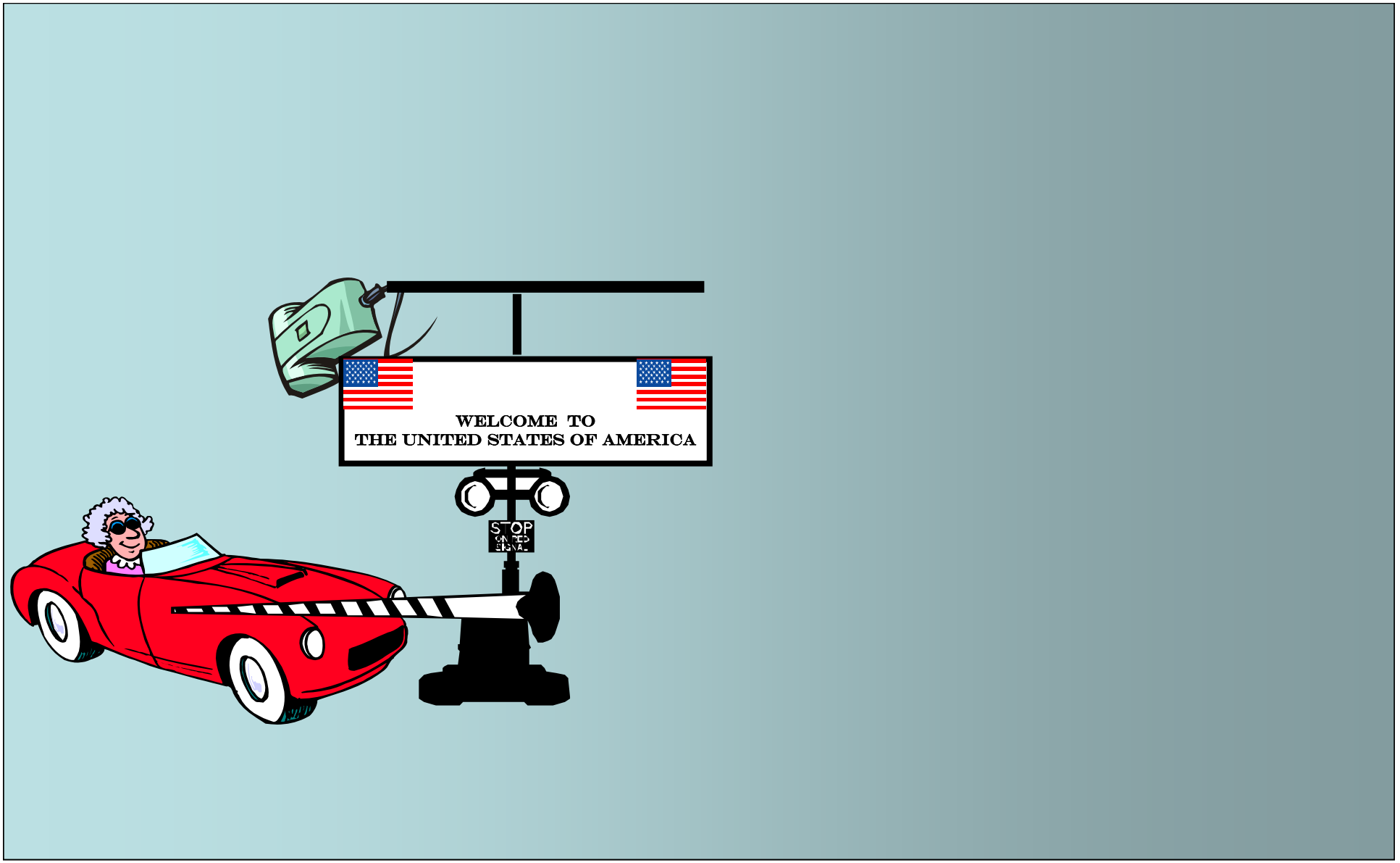
- <u>Design aim: Long read range</u>
- Other design aims?
  - Card cost?
  - Reader cost?

- Passport card is issued federally—for land and sea crossings only
- U.S. states are issuing drivers' licenses (EDLs) that can be used like passport cards
- WA was first…other border states followed

(Not to be confused with e-passport book…)



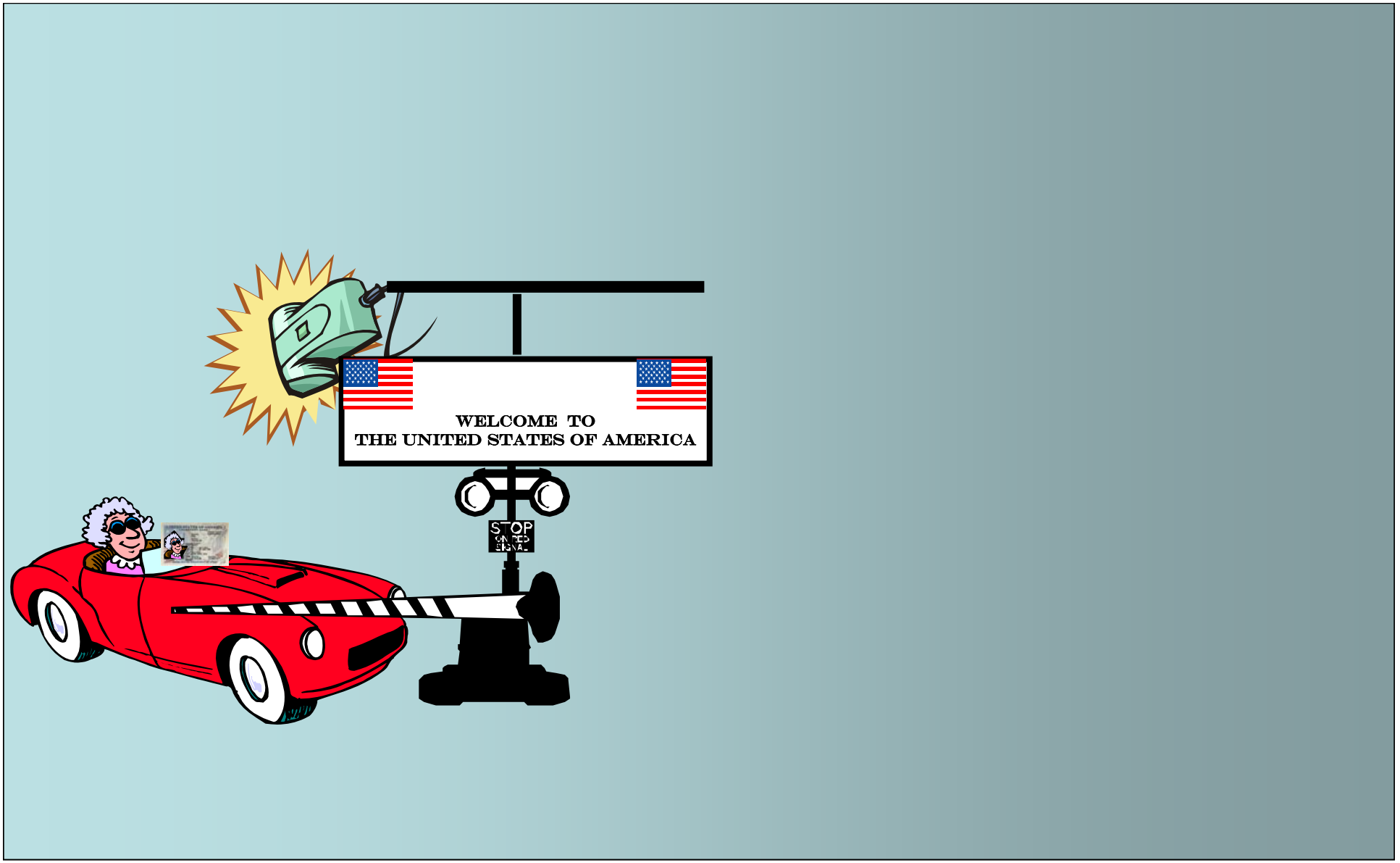
- Good for all international travel
- Reasonably good privacy protection
  - RF-opaque cover
  - “Basic access control,” i.e., cryptographic access control
  - Effective key length of about 52 bits for U.S.
    - (Juels, Molnar, and Wagner ’05)
  - Not too good for Netherlands and UK
- Biometric verification for anti-cloning
- Many problems in deployment…



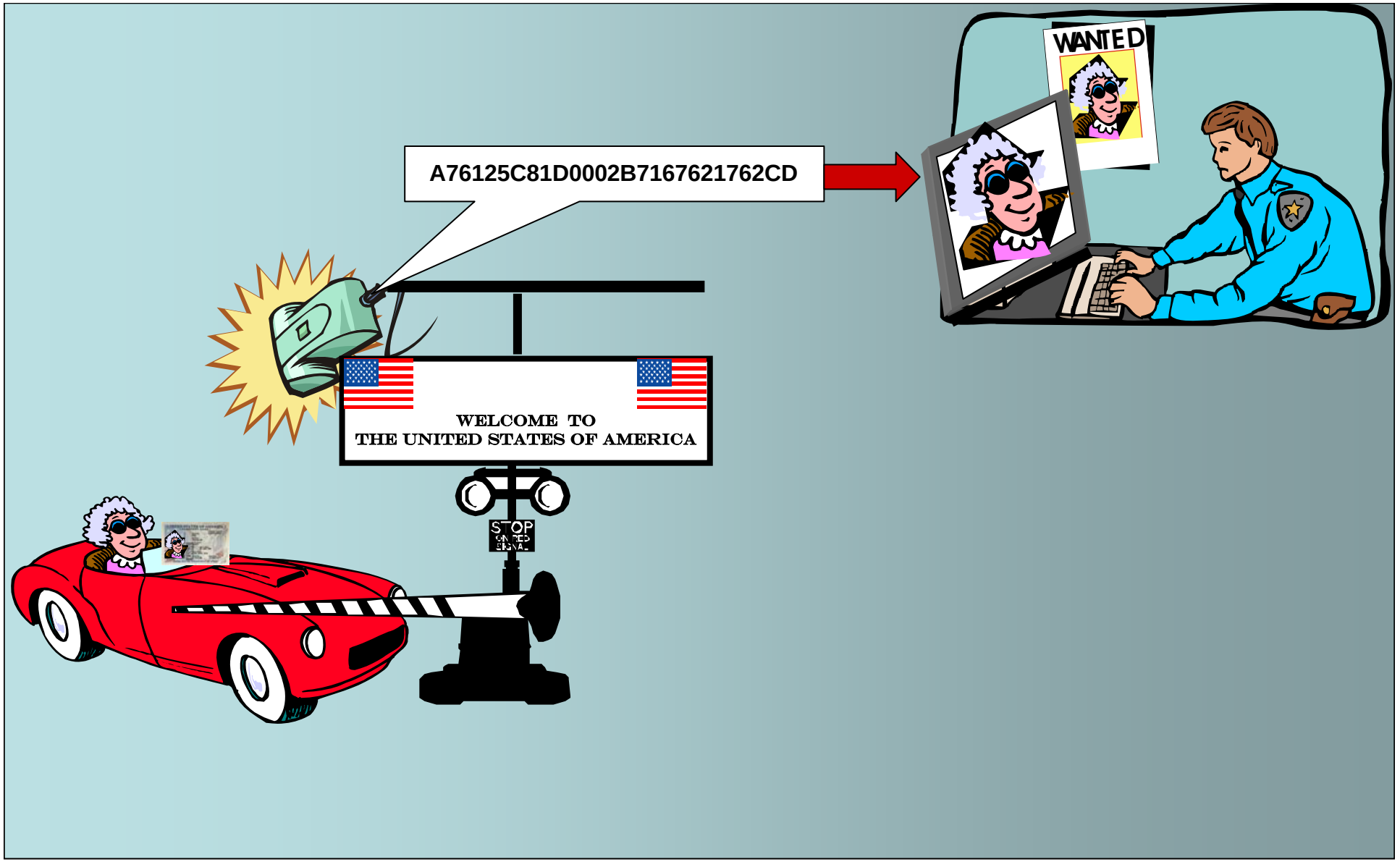
How does passport card work?



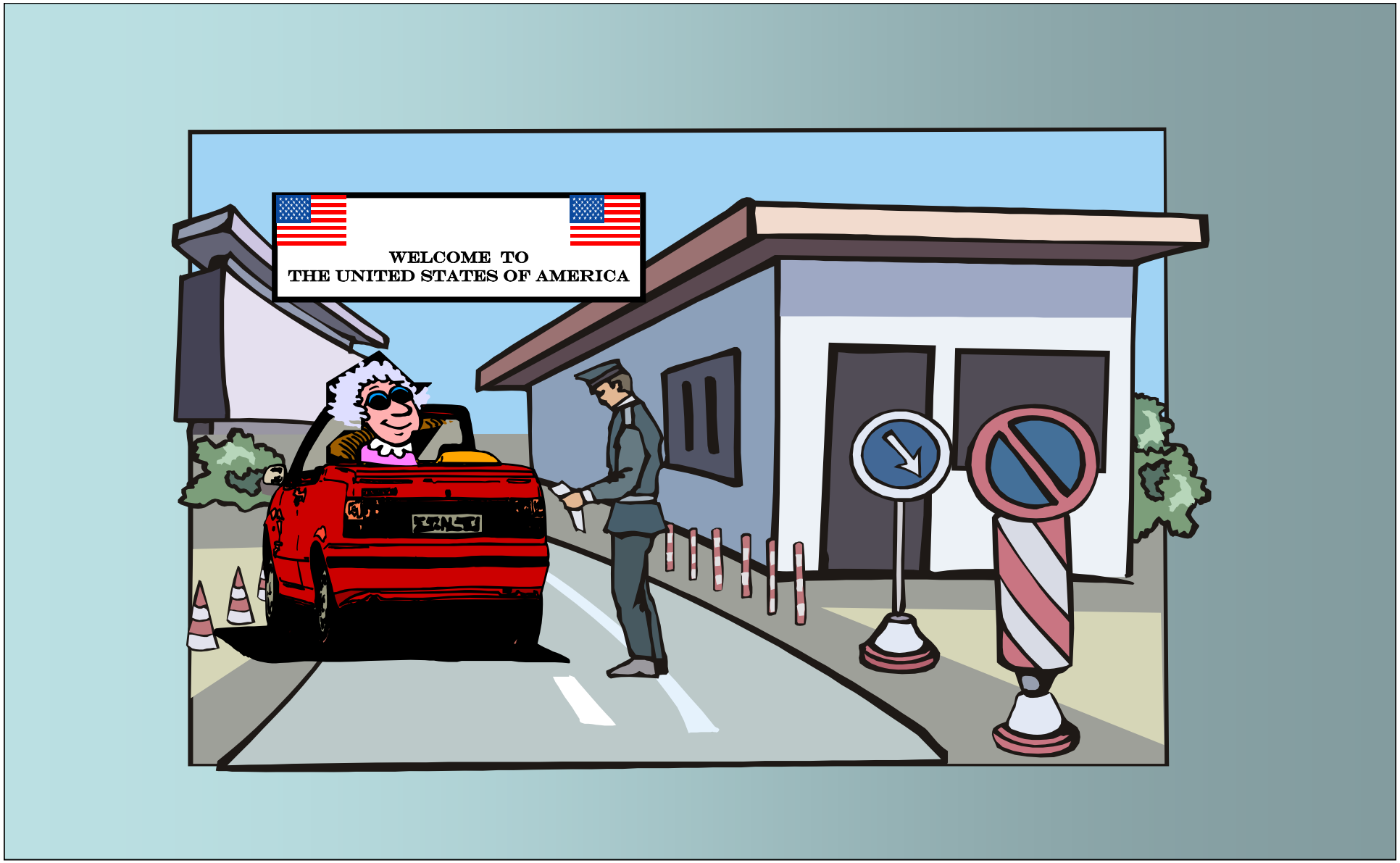
How does it work?



How does it work?

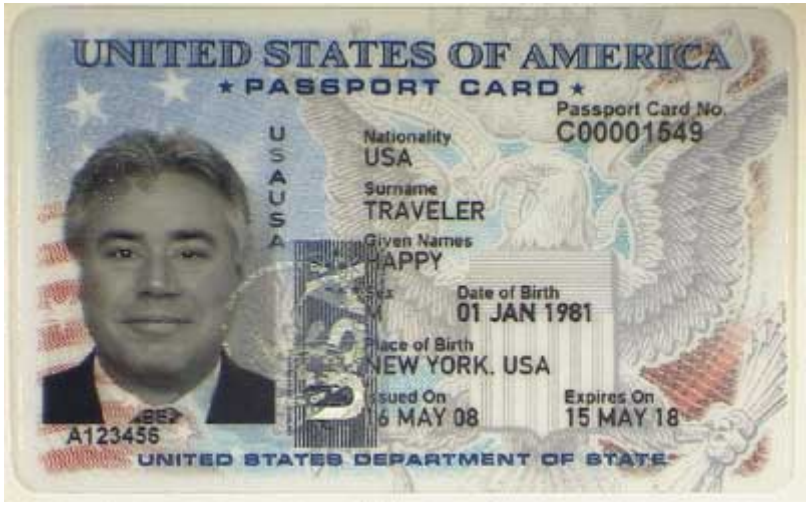


How does it work?



How does it work?

What’s the read range?



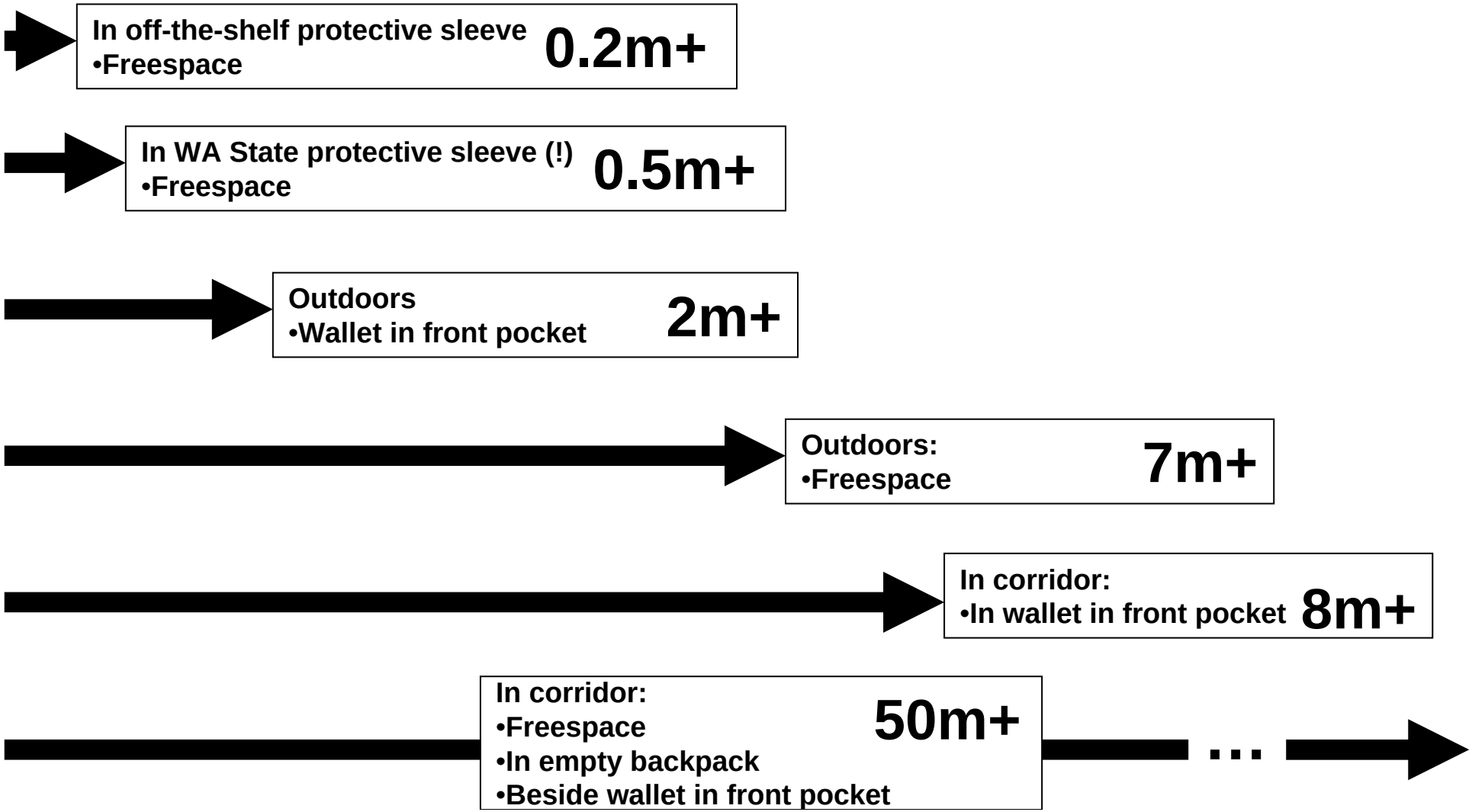
The border-crossing application requires good range (several meters)

More generally, a few things to consider:

- Again, the EPC tag is *passive*
- Water interferes with scanning of EPC tags
- People are mostly water
- The card is furnished with a protective sleeve—for removal only at border

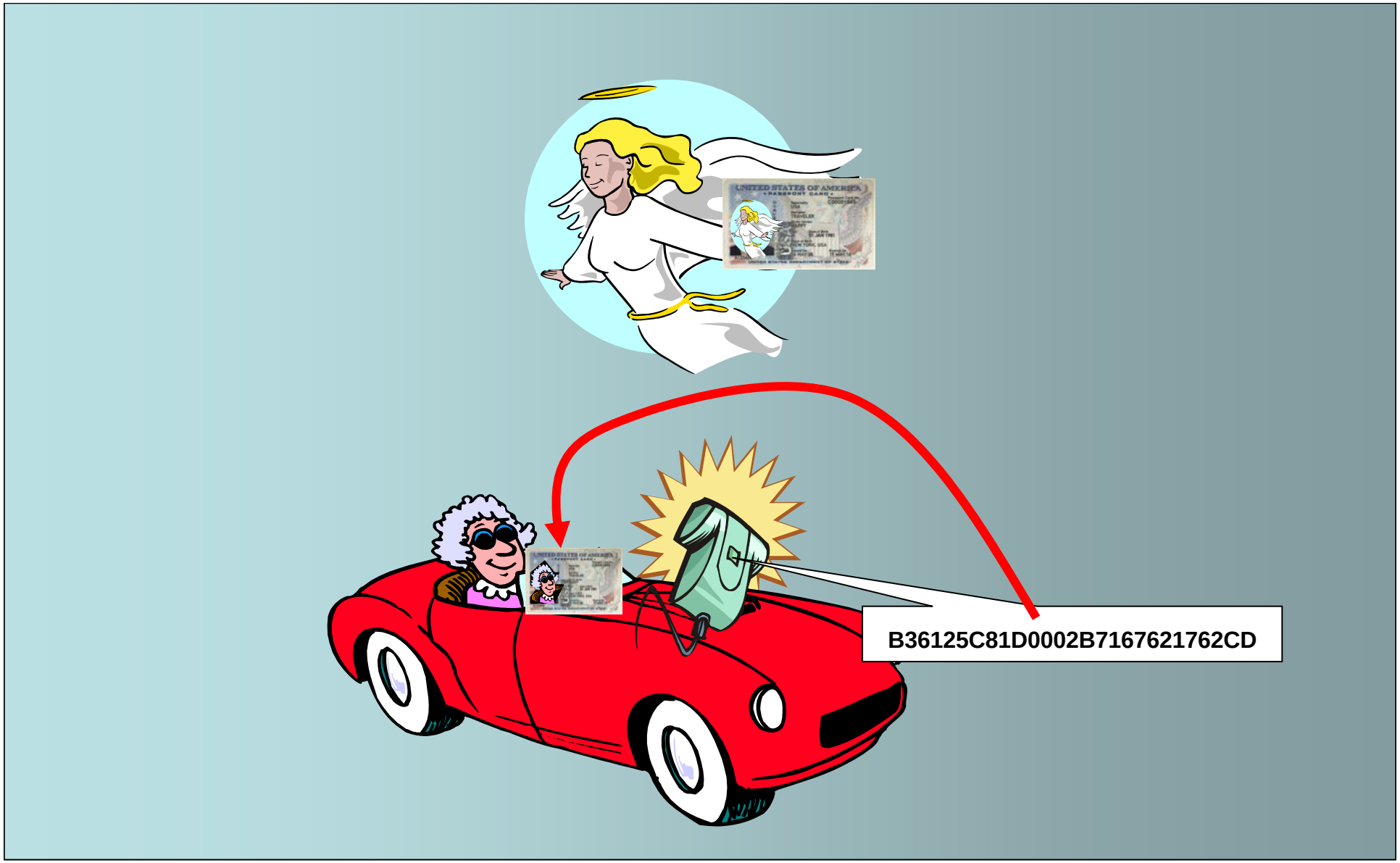
What's the read range?

(Figures for WA State EDL)

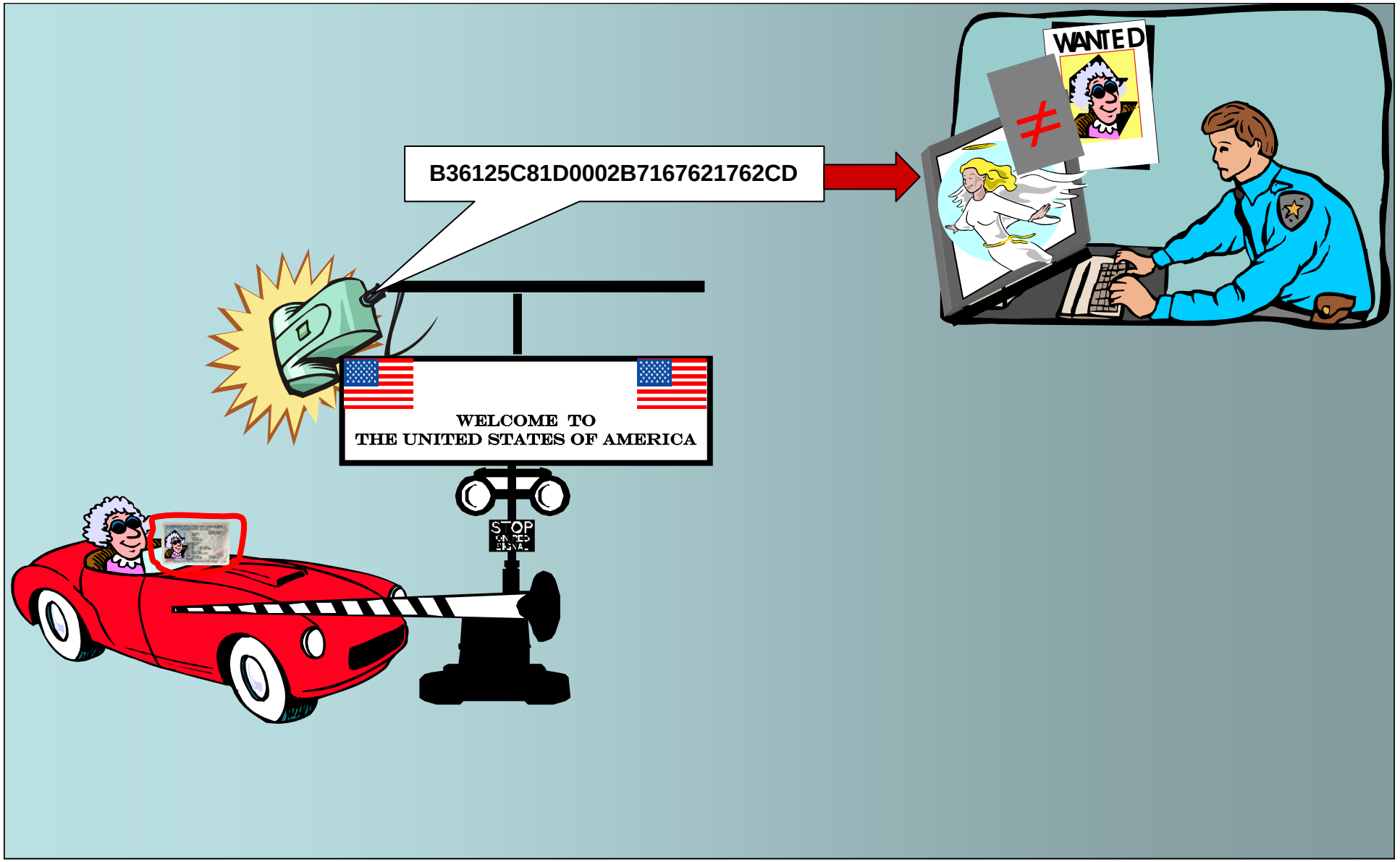


Why does this matter?

- EPC tags are easy to clone!
  - This is no secret or surprise… they're like barcodes!
- To read is to be able to clone
- We copied a passport card and EDL into off-the-shelf tags (e.g., a conference badge)
- U.S. Department of Homeland Security Privacy Impact Assessment described "tag ID" (TID) as a "powerful tool" for anti-counterfeiting
  - TID is serial number "burned in" by manufacturer
  - But easy to emulate in special-purpose device
  - Not present (as unique ID) in passport cards we examined!

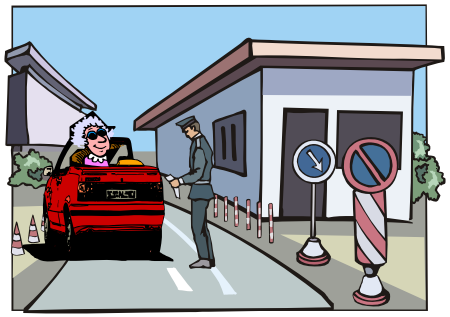


Reading suffices for cloning…



Cloned card means…

Is this fatal?



- Not necessarily: Remember protective sleeves and agent-interview step
- But remember too that people are people, subject to:
  1. Primacy effects
  2. Automation bias
  3. Vigilance decrement
     - E.g., privacy specialist who furnished our EDL had lost his/her protective sleeve
- And then there's design drift
  - E.g., WA State EDL could be killed over the air by anyone! (Kill PIN wasn't set!)

Is there any technical remedy?

- Remember, there are no explicit authentication features!
- There are two PINs in an EPC tag:
  - "Kill" PIN ***K***
  - Read / write access PIN ***K****
- "Poor man's" challenge-response using K^*:
  - Write secret value ***S*** to tag under K^*
  - Readable only under under K^*
  - Protects against rogue skimming of ***S***
  - Vulnerable to eavesdropping—but better than nothing!
- In the longer term: "Computational" RFID tags

A few concluding points

- RFID is a technology, not a specific device
- Security and privacy are subtle and application dependent
- Security challenge often a function not of on-board security features, but key management
- For more information, visit RFID CUSP www.rfid-cusp.com