PHILIPS

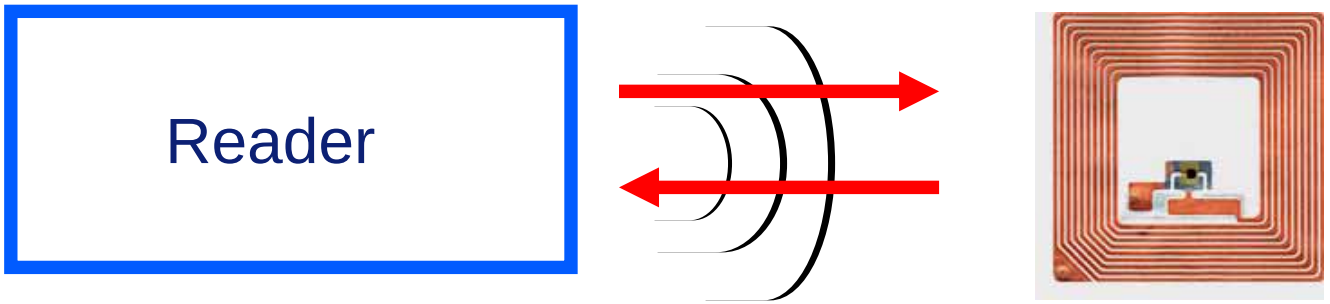
RFID-Tags: Privacy and Security Issues

P. Tuyls
Philips Research
pim.tuyls@philips.com

Overview

- RFID-Tags: What?
- Current, New and Emerging Applications
- Privacy Threat
- Security (Cloning) Threat
- Privacy Solutions
- Counterfeiting Solution
- Challenges

RFID-tags: What?



- Antenna connected to a micro-chip
- No battery, power is obtained from EM-field of the reader
- Low-cost identification of goods (Price: 1-2 cents -> 1$)
  - If no chip 1-2cents (billions pieces/year)
  - With chip 5 cents (billions/year)
- Next Generation Bar Codes: **no line of sight needed**
- Small: < $1mm^2$
- Range: up to several meters (depends on the frequency)

Current Applications

- Supply chain management: optimisations
- Automated inventory management,
- Automated quality control,
- Access control etc
- Ticketing and Payment Services…

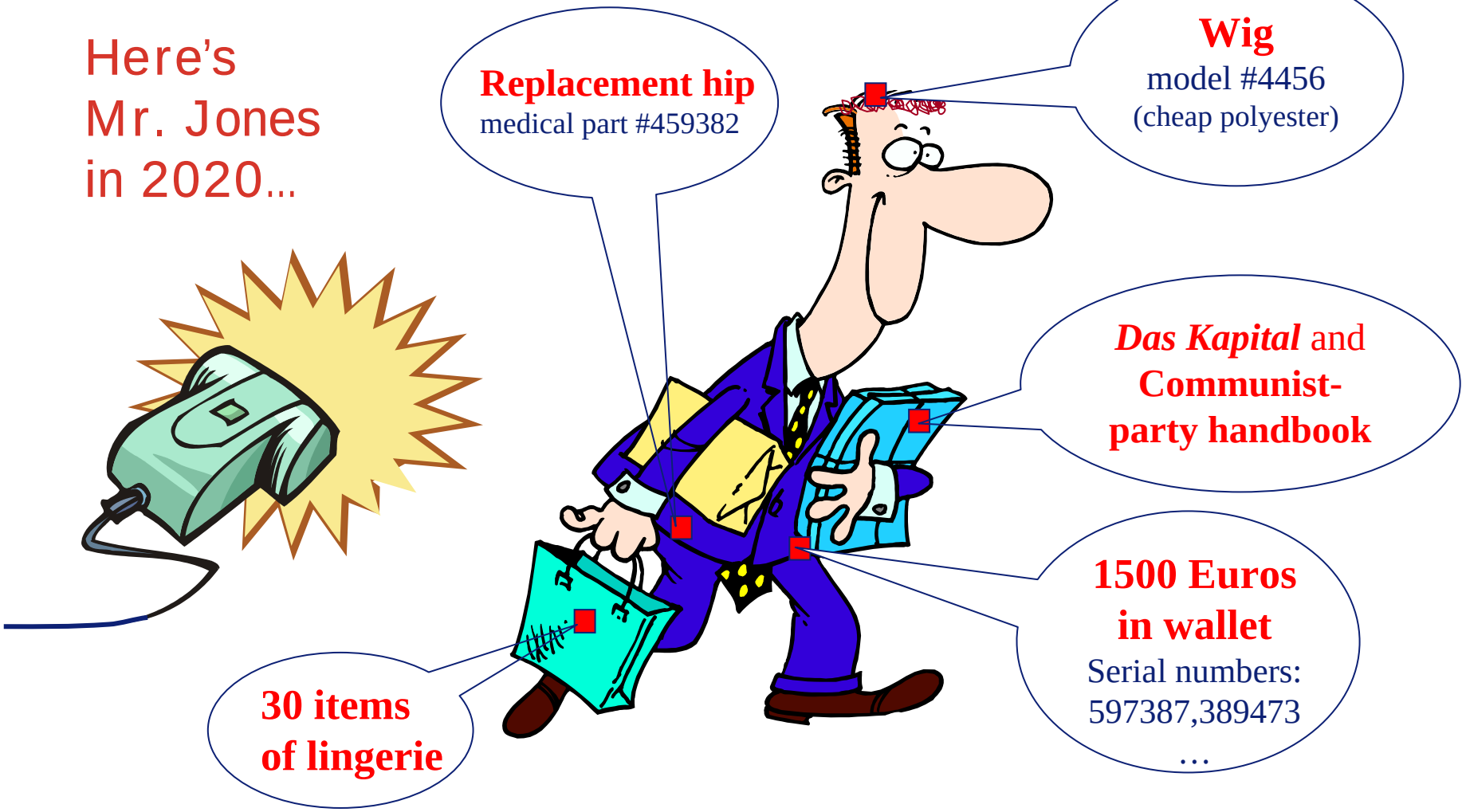
Assumption: Readers On-Line Connected with a database Realistic?

New and Emerging Applications

- **RFID-tags for new and personalized services**
  - RFID-Tags in Clothes
    - Intelligent washing machines
  - RFID-Tags in Food
    - Connected Fridges
  - RFID-Tags in Consumer Products
  - Protected Food Chain (from animal diseases)
  - Faster Shopping experience
- **RFID-Tags for Anti-Counterfeiting**
  - RFID-Tags on Medicines
    - Fake drugs kill!
  - RFID-Tags in Banknotes
  - RFID-Tags in Passports
  - RFID-Tags in high-valued goods

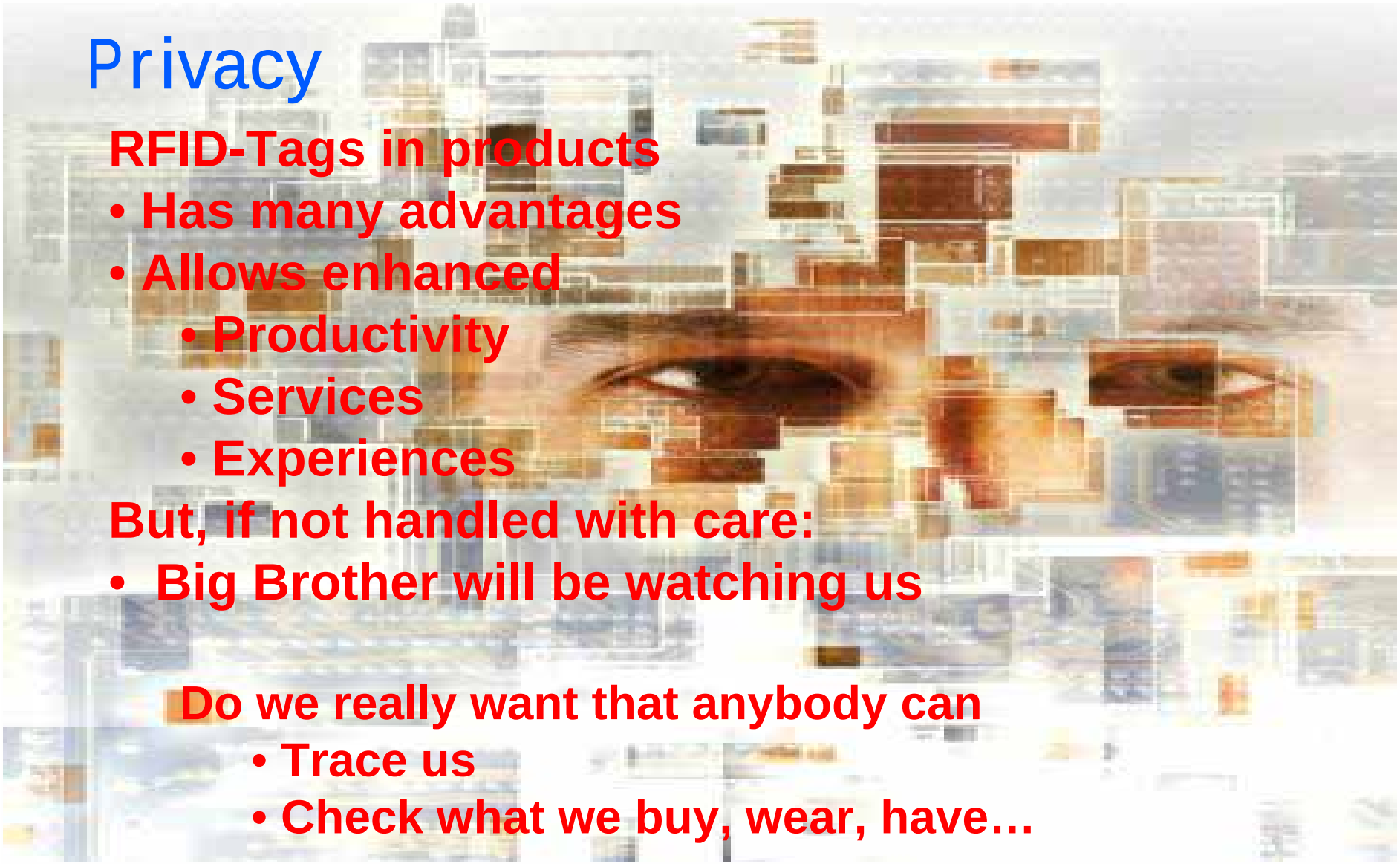
Threat 1: Privacy

Here's Mr. Jones in 2020…



* From a presentation by Ari Juels, USENIX Security 2004

Privacy



RFID-Tags in products

- **Has many advantages**
- **Allows enhanced**
  - **Productivity**
  - **Services**
  - **Experiences**

But, if not handled with care:

- **Big Brother will be watching us**

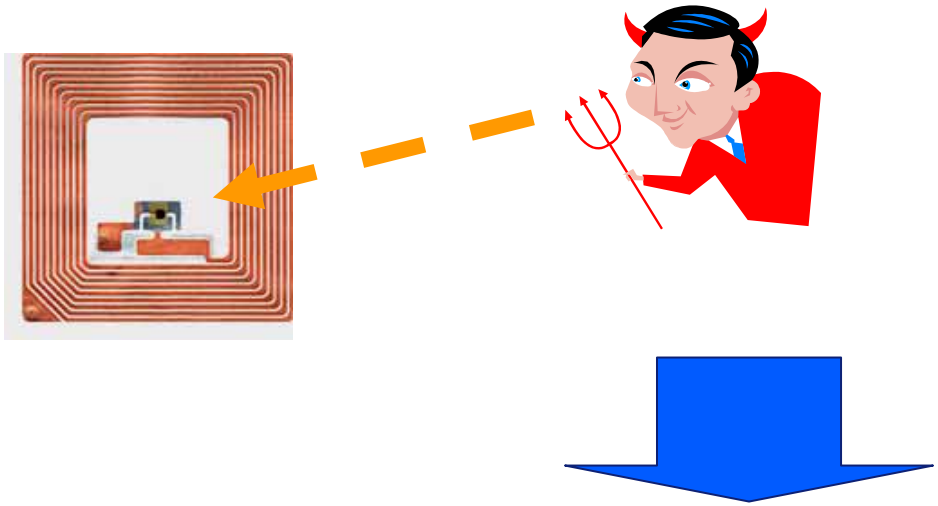
Do we really want that anybody can

- **Trace us**
- **Check what we buy, wear, have…**
- **…**

Threat 2: Security (Cloning)

- **Attacks on the security protocols (Active and Passive)**

- **Physical Attacks: Probing of the memory, Side Channel,…**



Attacker can derive the secret from the tag and make a clone

- E.g. EPC Tag is easily cloned (Basically a Barcode)

Solutions

Technological Solutions for

- **Privacy Threat**
- **Cloning Threat**

Two Components

- **Algorithms** (Encryption, Authentication, Secure ID, Digital Signatures,…)
- **Physics**
  - *Crypto-Physics*: Physics and Crypto integrated for a strong solution
  - *Physics*: Non-crypto security

Privacy Solutions

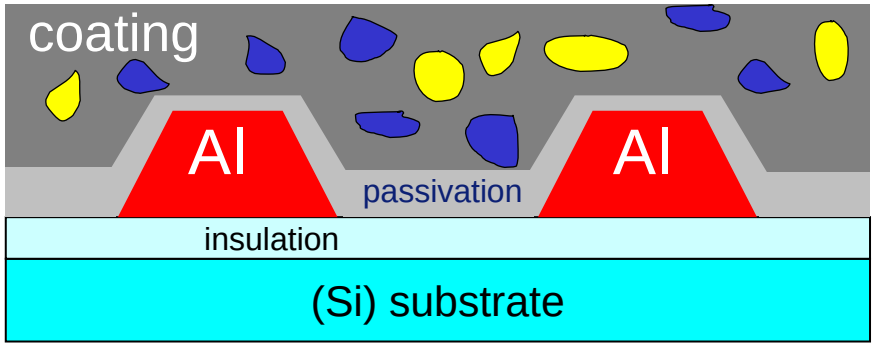
- Blocker Tag (Algorithm)
- Password Based (Algorithm)
  - Kill Command
- Updating of the Identifier of the Tag by the reader (Algorithm)
- Delay Solution (Algorithm)
  - Tag releases its data fast in the shop but keys slow
- Use Tag also as a Light Sensor (Physics)
  - Works only in an environment with sufficient light (not while in the banknote inside a wallet!)

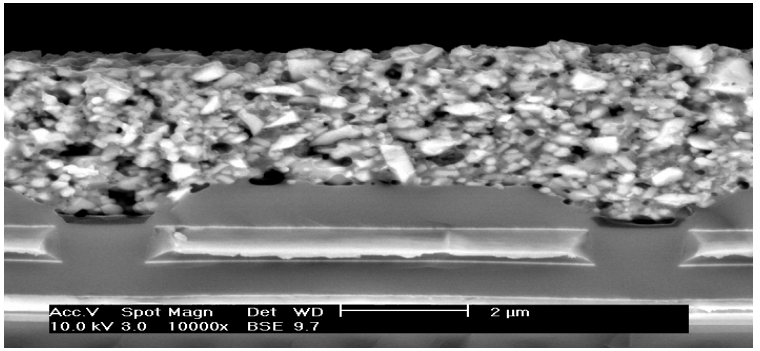
Anti-Counterfeiting Solution (CT-RSA06)

- **Embed RFID-tag in a product or its package**
  - Couple it with information (S/N, Value) on the package
- **Thwarting of the cloning attack: Unclonable RFID-Tag**
  - Combination of Physics and Crypto
    - Integrate an RFID-Tag with a Coating Physical Unclonable Function
  - Prevents Physical Attacks
  - Prevents Protocol Attacks

Coating PUF

- An IC is covered with an opaque coating containing random particles with high ε_r
- Array of capacitive sensors in upper metal layer detects local coating properties.
- Inhomogeneous coating → random capacitive properties

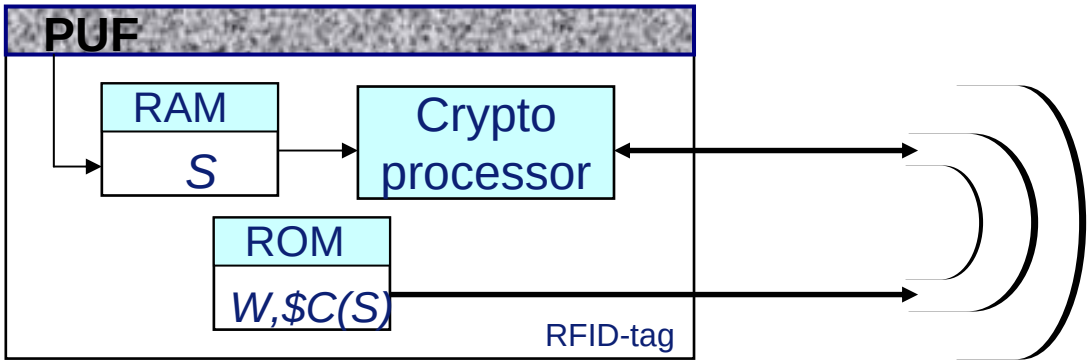




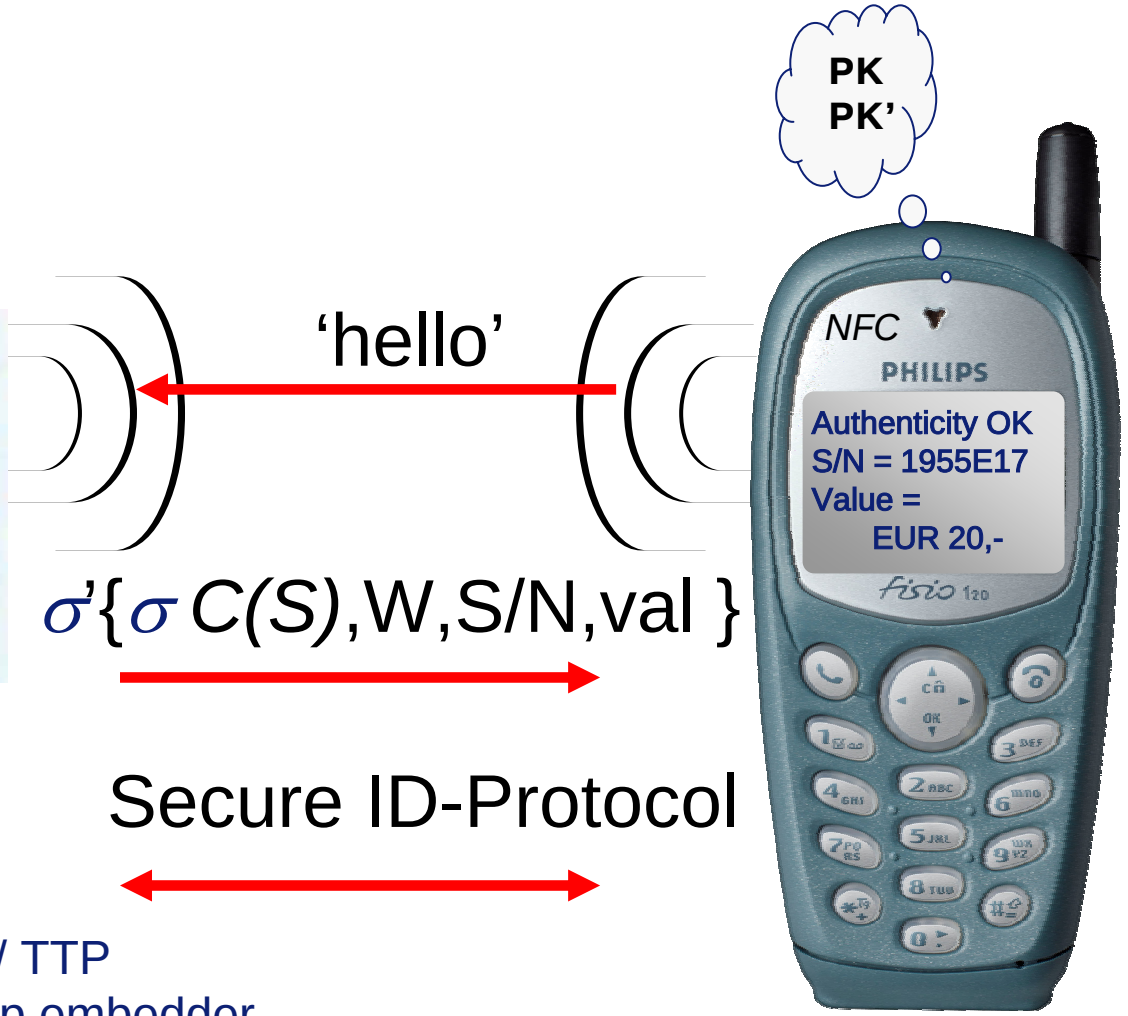
- PUF is used as a source of ***secret random information*** which are derived from the local coating capacitances (secure key storage).
- Damaged PUF leads to a destroyed key

Unclonable RFID tag

- RFID-tag equipped with a coating PUF
  - Removing the PUF leads to destruction
  - Attacker can not tamper with the communication between PUF and tag
  - PUF-output is inaccessible to an attacker
- A unique, secret bit-string *S* is derived from the Coating PUF.
  - (helper data/Fuzzy Extractor)
- *S* is only temporarily in volatile memory
- Reference information $\sigma(C(S))$: *commitment* to *S*, *signed* by TTP and stored in ROM.
- *Aux data:* *produced by the Fuzzy Extractor*: W



Protocol



PK = public key of chip producer / TTP
PK' = public key of customer / chip embedder
S/N = serial number

Note: Verification is performed Off-line!

RFID-Based Solution: PUF-Cert-ID Based ID Protocol

- **Basic Components:**
  - PUF,
  - Fuzzy Extractor: (G,J),
  - SS: (SK_g, Sign, V_f),
  - SI: (K_g, P,V)

- **New Scheme:**
  - (MK_g, Uk_g, **P**,**V**)

- **Enrollment**

  – Identity: id-number of the tag; e.g. serial number
  – Uk_g -> (sk, pk); MK_g <- SK_g
  – For c, x(c) -> compute w such that from x(c) and w=J(x(c),sk):
    sk can be generated (on the tag, w is stored in ROM, sk is not stored!)
  – Cert <- (pk, Sign(msk, pk||I)); Usk <- (PUF,Cert)

- **Authentication**

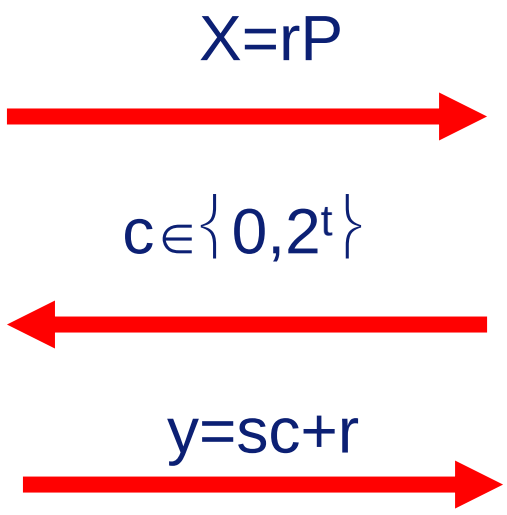
  – PUF is challenged: y(c), Tag computes from y(c) and w:
    sk=G(y(c),w)
  – Cert is checked
  – SI is run on pk

Implementation

- Secure ID-Protocol
  - Schnorr on an ECC over GF(2^{163})

Prover
Secret: sk=s

Verifier
Public: pk=-sP



Verifies:
yP+cV=X

Feasibility

Computational cost

- PUF: Noisy Measurements: error correction is needed
  - Price: 1000 gates (Decoding algorithm)
- Schnorr Identification Protocol
  - Price: 1 Mult on ECC: 3000 gates (estimate)
- Other overhead: 1000 gates
- Total 5000 gates

Storage cost

- sP, c, (sP): ECDSA: 489 bits

Shows that PK-Crypto is Feasible on a Tag!

Security

- Coating PUF can not be cloned
- Since S does not leak from the tag: breaking the anti-counterfeiting protocol implies:
  - *Breaking the Signature Scheme*
  - *Breaking the Secure Identification Protocol*
  - *Breaking the Fuzzy Extractor for the PUF*

Challenges

- Crypto and Security Algorithms for constrained devices
  - Even more Efficient Symmetric Key Algorithms
    - Understand how trade-offs have impact on security
  - Public Key algorithms for a Tag
    - Optimise for Area and power, not for Speed
    - Look at ECC and HECC
    - Tune algorithms to the required security level of an application
  - More fundamentally: Try to build up understanding of what is ultimately possible in a constrained environment
- Automatic verification tools
  - Verify the security/Privacy of protocols

Conclusions

- RFID-Tags:
  - Support many nice applications
  - Integration with Privacy Preserving Technology to prevent a Big Brother Society
  - Crypto Solutions
  - Physics Based Solutions

- Unclonable RFID-Tags for Anti-Counterfeiting
  - Needed!
  - Crypto-Physics

- Get deeper understanding of classical crypto algorithms
  - Understand how trade-offs have impact on security
  - Develop light versions